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:

DFAS Contract Debt System (DCDS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

06/15/20

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.

Debts owed to the DoD by contractors are maintained in the Defense Finance and Accounting Service (DFAS) Contract Debt System (DCDS) through the Contractor offset program (COP) which allows input of debt detail, debt letter generation and email notification, accounts receivable recording of collections and generation of collection memos identifying which lines to Intra-Governmental Payments and Collections (IPAC) the funds, tracking by aging, status and interest, as well as monthly debt management reporting.
DCDS contains information unique to contractors, and information unique to contractor hospital patients cared for in DoD hospitals, including social security numbers.

The type of PII in DCDS is: Employment Information, Home/Cell Phone, Mailing/Home Address, Race/Ethnicity, Work E-mail Address, Birth Date, Financial Information, Personnel E-mail Address, DoD ID Number, Name(s) and Social Security Number (SSN) (Full or in any form), employee identification number, and data universal numbering system number for contractors .

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)*

DCDS uses PII for identification for the billing process.

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

DCDS does not collect PII directly from any individual

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

DCDS does not collect PII information directly from any individual.

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
- [x] Not Applicable

DCDS does not collect PII information directly from any individual.

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

[X]	Within the DoD Component	Specify.	PII will be shared on a need to know basis with internal DFAS accounting organizations
[ ]	Other DoD Components	Specify.	
[X]	Other Federal Agencies	Specify.	PII will be shared on a need to know basis with the Department of Treasury for the Defense Treasury Offset Program (DTOP).
[ ]	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.	
[ ]	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
- [ ] Databases
- [X] Existing DoD Information Systems
- [ ] Commercial Systems
- [ ] Other Federal Information Systems

DCDS collects PII from existing DoD information systems that handle PII, such as the Wide Area Work Flow (WAWF). Users also key in data related to contractor debts, and import files related to medical billings.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Face-to-Face Contact
- [ ] Paper
- [ ] Fax
- [ ] Telephone Interview
- [X] Information Sharing - System to System
- [ ] Website/E-Form
- [X] Other *(If Other, enter the information in the box below)*

DCDS collects PII from existing DoD information systems that handle PII, including WAWF. Users also key in data related to contractor debts, and import files related to medical billings. Users do not key in PII but may include attachments, ie; a copy of the SAM for each Vendor that contains phone numbers, email addresses, EIN and DUNS# for contractors.

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier T7800

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 TBD

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.

Records are retained according to DFAS records retention schedule; cut-off on date of final action destroy 10 years after cut-off; hard copy reports are sent to LAN printers and cover sheets are used to protect data. The general guidelines references are DFAS Records Management Procedures, 5015.2-I and DFAS Records Disposition Schedule, 5015.2-M.

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.

31 U.S.C. 3512, Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R Vols. 6A and 6B, and E.O. 9397 (SSN) as amended. Federal agencies or non-Federal agencies as regulated by the Privacy Act of 1974 (5 U.S.C. 552a), as amended. DCDS supports the Centralized Offset Program (COP) which allows for the collection of debts from invoice being paid to the debtors.

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.

Per DFAS Agency Information Management Control Officer (IMCO), Agency Program Management Office, Support Services, this system does not require an OMB approval number because it does not collect information directly from the public, and the feeder systems require approval which gives DCDS the ability to go forward without those approvals.

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	

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.

Currently updating SSN justification memo for CIO signature, will forward to DFAS Privacy Office for submission to DPCLTD for approval.

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

The justification for the use of the SSN and/or TINs is Department of Defense (DoD) Instruction 1000.30, "Reduction of Social Security Number (SSN) Use within DoD", dated August 1, 2012, Enclosure 2, Paragraph 2.c. (7) "Federal Taxpayer Identification Number". The application of Federal and State income tax programs rely on the use of the SSN and TIN. As such, systems that have any function that pertains to the collect, payment, or record keeping of this use may contain the SSN and TIN. Additionally, individuals who operate business under their own name may use their SSN as the tax identification number for the business entity.

(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".

Unable to mitigate as the data is required to track billing/debt DCDS must continue to use the SSN/TIN for record identification.

(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

There is no plan to eliminate the use of the SSN/TIN, due to the need to identify medical information for bill/debt processing.

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)*

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

System inherits all physical, technical and administrative controls protecting DFAS Enterprise Local Area Network (ELAN) where system is hosted.

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

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

N/A

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

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

N/A

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

N/A

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]?

[X]	Yes, DITPR	DITPR System Identification Number	DITPR ID 17264
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	101
[ ]	No		

If "No," explain.

N/A

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:

[X]	Authorization to Operate (ATO)	Date Granted:	11/22/2017
[ ]	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.

Tri-Annual Authorization scheduled for renewal/completion 11/21/2020

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

N/A

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 [X] No

If "Yes," Enter UII [ ] If unsure, consult the component IT Budget Point of Contact to obtain the UII

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

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Kenna Robinett	(1) Title	System Manager
(2) Organization	DFAS-CO-JBMBA, System Operations	(3) Work Telephone	614.701.2451
(4) DSN	791.2451	(5) E-mail address	kenna.m.robinett.civ@mail.mil
(6) Date of Review	11/14/19	(7) Signature	ROBINETT.KENNA.M.1230182759 Digitally signed by ROBINETT.KENNA.M.1230182759 Date: 2019.11.25 12:25:59 -05'00'
b. Other Official *(to be used at Component discretion)*	David M. Glover II, MBA	(1) Title	Director, Columbus
(2) Organization	DFAS-CO-JBM, Accounting System	(3) Work Telephone	614.701.4810
(4) DSN	791.4810	(5) E-mail address	david.m.glover4.civ@mail.mil
(6) Date of Review	12/04/19	(7) Signature	GLOVER.DAVID.M.III.1041475524 Digitally signed by GLOVER.DAVID.M.III.1041475524 Date: 2019.12.04 11:13:49 -05'00'
c. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
d. Component Privacy Officer (CPO)	Gregory L. Outlaw	(1) Title	Privacy Officer
(2) Organization	DFAS-ZC, Corporate Communications	(3) Work Telephone	317.212.4591
(4) DSN	699.4591	(5) E-mail address	gregory.l.outlaw.civ@mail.mil
(6) Date of Review	02/05/20	(7) Signature	OUTLAW.GREGORY.L.1085047317 Digitally signed by OUTLAW.GREGORY.L.1085047317 Date: 2020.02.05 12:49:40 -05'00'

e. Component Records Officer	Ralph Mullins	(1) Title	Agency Records Manager
(2) Organization	DFAS-IN, ZED	(3) Work Telephone	317.212.7775
(4) DSN	699.7775	(5) E-mail address	ralph.e.mullins.civ@mail.mil
(6) Date of Review	02/06/20	(7) Signature	MULLINS.RALPH.EDWARD.JR.1059546534 Digitally signed by MULLINS.RALPH.EDWARD.JR.1059546534 Date: 2020.02.06 10:11:36 -05'00'
f. Component Senior Information Security Officer or Designee Name	Jack Schiller	(1) Title	Acting Director, IT Shared Services
(2) Organization	DFAS-ZTA	(3) Work Telephone	317.212.1808
(4) DSN	699.0018	(5) E-mail address	jack.j.schiller.civ@mail.mil
(6) Date of Review:	05/26/20	(7) Signature	SCHILLER.JACK.JOSEPH.1457280200 Digitally signed by SCHILLER.JACK.JOSEPH.1457280200 Date: 2020.05.27 23:58:45 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Angela R. Schultz	(1) Title	Director, Corporate Communications
(2) Organization	DFAS-ZC	(3) Work Telephone	317.212.6195
(4) DSN	699.6195	(5) E-mail address	angela.r.schultz6.civ@mail.mil
(6) Date of Review	03/04/20	(7) Signature	SCHULTZ.ANGELA.RENAE.1230338309 Digitally signed by SCHULTZ.ANGELA.RENAE.1230338309 Date: 2020.03.04 10:17:24 -05'00'
h. Component CIO Reviewing Official Name	G. Paul Gass	(1) Title	Director, Information Technology
(2) Organization	DFAS-ZT	(3) Work Telephone	317.212.4800
(4) DSN	699.4800	(5) E-mail address	gregory.p.gass2.civ@mail.mil
(6) Date of Review	06/15/20	(7) Signature	GASS.GREGORY.PAUL.II.1109700440 Digitally signed by GASS.GREGORY.PAUL.II.1109700440 Date: 2020.06.15 13:48:55 -04'00'

Publishing: Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.