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:

Defense Business Management System (DBMS)

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

07/15/20

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.

DBMS will provide a means of reporting all costs entering the general ledger; account for appropriated funds; provide a means of reconciling financial records and for the preparation of most financial reports. Records will be used for extraction or compilation of data and reports for management studies for use internally or externally as required by Department of Defense (DoD) or other government agencies such as the Department of the Treasury. Personal Information maintained in the system consists of individual's name and Social Security Number (SSN).

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)*

To update individuals entitlements for Defense Agencies lines of accounting which are used to produce financial reports for DoD.

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.

DBMS does not collect PII data directly from individuals. It receives data from the Defense Civilian Payroll System (DCPS) and Defense Travel System (DTS) for the posting and accounting of personnel and travel expenses.

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.

DBMS does not collect PII data directly from individuals. It receives data from the Defense Civilian Payroll System (DCPS) and Defense Travel System (DTS) for the posting and accounting of personnel and travel expenses.

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

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 only be shared within DFAS Accounting Operations.
[X]	Other DoD Components	Specify.	Defense Commissary Agency (DeCA)
[X]	Other Federal Agencies	Specify.	Department of Treasury
[ ]	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
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

Defense Civilian Payroll System (DCPS) and Defense Travel System (DTS).

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
- [X] 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

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 T7205a

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.

Records are retained according to DFAS records retention schedule. Hard copies of 'Screen Prints' are protected in accordance with DFAS procedures for protecting sensitive information. Operations will be reminded of their responsibilities to protect PII particularly when hard copies exist.

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., Chapter 35, Accounting & Collection; 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.

DBMS does not collect PII data directly from individuals. It receives data from the Defense Civilian Payroll System (DCPS) and Defense Travel System (DTS) for the posting and accounting of personnel and travel expenses.

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.

In the process of preparing SSN Justification Memo for CIO approval and submission to DOD Privacy Office for final 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 use of SSN for DCPS is based on compliance with DoDI 1000.30; 1) DoDI 1000.30, Enclosure 2, Paragraph 2.c (7) "Federal Tax Payer Identification Number". 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".

Due to last remaining customer, DeCA, scheduled to migrate to Defense Agencies Initiative (DAI) effective Oct 1, 2020, there is no effort to reduce the use of SSN.

(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

Due to last remaining customer, DeCA, scheduled to migrate to DAI effective Oct 1, 2020, there is no plan to eliminate the use of SSN or mitigate its use.

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

System inherits all physical controls protecting DISA DECC hosting enclave in Ogden, Utah. DISA asserts to these controls in the delivery of their "Service Organization Controls 1 Report: Description of the System Supporting the Delivery of Hosting Services Provided by Defense Information Systems Agency (DISA) Hosting Services, For the Period from 01 October 2018 to 30 June 2019"

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

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

DBMS is on a DISA DECC enclave and may not be encrypted for operational reasons, but they are subject to layered protective measures determined to be adequate for sensitive unclassified information. System inherits all administrative controls protecting DISA DECC hosting enclave in Ogden, Utah.

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

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

System inherits all technical controls protecting DISA DECC hosting enclave in Ogden, Utah. DISA asserts to these controls in the delivery of their "Service Organization Controls 1 Report: Description of the System Supporting the Delivery of Hosting Services Provided by Defense Information Systems Agency (DISA) Hosting Services, For the Period from 01 October 2018 to 30 June 2019".

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

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	15
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	60
[ ]	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:

[X]	Authorization to Operate (ATO)	Date Granted:	9/10/2019
[ ]	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?

[X] Yes [ ] No

If "Yes," Enter UII 007-97-01-01-02-0568-00 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.

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	Dorothea Jenkins	(1) Title	System Manager
(2) Organization	DFAS-CO	(3) Work Telephone	614-701-2151
(4) DSN		(5) E-mail address	dorothea.jenkins.civ@mail.mil
(6) Date of Review	03/05/20	(7) Signature	JENKINS.DOROTHEA.1127564511 Digitally signed by JENKINS.DOROTHEA.1127564511 Date: 2020.03.05 12:53:20 -05'00'
b. Other Official *(to be used at Component discretion)*	Kristina L. Krebs	(1) Title	Accounting Services Director
(2) Organization	ZTC Accounting Services	(3) Work Telephone	216-204-3327
(4) DSN		(5) E-mail address	Kristina.L.Krebs.civ@mail.mil
(6) Date of Review	05/11/20	(7) Signature	KREBS.KRISTINA.L.1251897170 Digitally signed by KREBS.KRISTINA.L.1251897170 Date: 2020.05.11 21:00:32 -04'00'
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-IN/ZCF	(3) Work Telephone	317-212-4951
(4) DSN	699-4951	(5) E-mail address	gregory.l.outlaw.civ@mail.mil
(6) Date of Review	07/10/20	(7) Signature	OUTLAW.GREGORY.L.1085047317 Digitally signed by OUTLAW.GREGORY.L.1085047317 Date: 2020.07.10 14:39:46 -04'00'

e. Component Records Officer	Ralph Mullins	(1) Title	Agency Records Manager
(2) Organization	DFAS-IN/ZED	(3) Work Telephone	317-217-7775
(4) DSN	699-7775	(5) E-mail address	ralph.e.mullins.civ@mail.mil
(6) Date of Review	07/13/20	(7) Signature	MULLINS.RALPH.EDWARD.JR.1059546534 Digitally signed by MULLINS.RALPH.EDWARD.JR.1059546534 Date: 2020.07.13 08:11:30 -04'00'
f. Component Senior Information Security Officer or Designee Name	Jack Schiller	(1) Title	Deputy Director, IT Shared Services
(2) Organization	DFAS-IN/ZTA	(3) Work Telephone	317-212-1808
(4) DSN	699-1808	(5) E-mail address	jack.j.schiller.civ@mail.mil
(6) Date of Review:	07/13/20	(7) Signature	SCHILLER.JACK.JOSEPH.1457280200 Digitally signed by SCHILLER.JACK.JOSEPH.1457280200 Date: 2020.07.13 16:43:18 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Angela Schultz	(1) Title	Director, Corporate Communications
(2) Organization	DFAS-IN/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	07/13/20	(7) Signature	SCHULTZ.ANGELA.RENAE.E.1230338309 SCHULTZ.ANGELA.RENAE.E.1230338309 2020.07.13 08:28:35 -04'00'
h. Component CIO Reviewing Official Name	Gregory Paul Gass	(1) Title	Director, Information Technology
(2) Organization	DFAS-IN/ZT	(3) Work Telephone	(317) 212-1161
(4) DSN	699-1161	(5) E-mail address	gregory.p.gass2.civ@mail.mil
(6) Date of Review	07/15/20	(7) Signature	GASS.GREGORY.PAUL.II.1109700440 Digitally signed by GASS.GREGORY.PAUL.II.1109700440 Date: 2020.07.15 15:16:34 -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.