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:

One Pay

2. DOD COMPONENT NAME:

Defense Finance and Accounting Service

3. PIA APPROVAL DATE:

11/23/20

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
- ☒ 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.

One Pay is an on-line vendor payment system. One Pay provides invoice tracking, on-line inquiry, invoice status, and disbursing reports. This information is obtained from file transfers from the accounting and pay entitlement systems. The type of personal information collected is the individual's: address, home phone number, bank routing/account number, other ID - corporate Employee Identification Number/Tax identification Numbers (EIN/TINs), name, alternate ID, and Social Security Numbers (SSN) for Defense Finance and Accounting Service (DFAS) payees.

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)*

Personally Identifiable Information (PII) is used in order for the Defense Agencies and their authorized support personnel to identify, verify, and authenticate personnel information in order to assist in proper payments.

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.

One Pay does not collect PII directly from the individual.

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.

One Pay does not collect PII directly from the 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 ☒ Not Applicable

One Pay does not collect PII directly from the 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.	DFAS Accounts Payable Operations located in Indianapolis, IN; Cleveland, OH; Rome, NY; and Japan.
[X] Other DoD Components	Specify.	Navy and Marine Corps customers.
[X] Other Federal Agencies	Specify.	United States Department of Treasury and Internal Revenue Service (IRS). Information may be shared with the Department of Justice for investigative purposes.
[ ] 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 Travel System (DTS), Integrated Management Processing System (IMPS), Naval Research Laboratory (NRL), Naval Education and Training Professional Development Center (NETPDTC), Navy Marine Corps Intranet (NMCI), Navy Reserve Order Writing System (NROWS), Third Party Payment System (TPPS-T), Invoice, Receipt, Acceptance and Property Transfer (iRAPT), Defense Industrial Financial Management System (DIFMS), Defense Integrated Financial System (DIFS), Defense Working Capital Fund Accounting System (DWAS), Government Travel System (GTS), Standard Accounting and Reporting System (STARS), Standard Accounting, Budgeting, & Reporting System (SABRS).

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.

[ ] Yes [X] 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://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.

One Pay data is not researchable by PII.

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. Rule 4, Schedule 7206, DF

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

(3) Retention Instructions.

Cut off at the end of the fiscal year in which all obligations of the closed account are liquidated. Destroy 10 years after cutoff. AUTH: (GRS 1.1, Item 010)

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.

Executive Order 9397 (as amended) authorized solicitation and use of the Social Security Number (SSN) as a numerical identifier for Federal personnel who are identified in most Federal record systems. See Executive Order 12862, dated September 11, 1993; and DoD Financial Management Regulation 7000.14-R, Volume 5.

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.

One Pay does not collect PII directly from individuals 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	

Other is for Corporate Employee Identification Number/Tax identification Numbers (EIN/TINs) which is a unique identification number that is assigned to a business entity so that it can easily be identified by the Internal Revenue Service (IRS).

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.

Signed by Cindy Allard, DPCLTD, on 3 April 2019.

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

DoD Instruction 1000.30, Enclosure 2, Section 2c.(7), Federal Taxpayer Identification Number, which states,"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".

SSN are masked/redacted.

(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

One Pay will maintain the SSN as part of its data inventory until the IRS uses a different unique identifier for issuing tax documentation.

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
- [ ] Closed Circuit TV (CCTV)
- [x] Identification Badges
- [ ] Safes
- [ ] If Other, enter the information in the box below

One Pay is located within the Defense Information Systems Agency (DISA) enclave and is subject to layered protective measures determined to be adequate for sensitive unclassified information. One Pay inherits all DISA Data Center administrative controls protecting DISA Data Center hosting enclave and the Defense Finance and Accounting Services (DFAS) Enterprise Local Area Network (ELAN) where developers, users, and system administrators are located.

(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
- [ ] If Other, enter the information in the box below

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

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

One Pay roles that allow users to access any PII information, requires One Pay Project Management Office (PMO) approval before an Information System Security Officer (ISSO) can grant any user this access. Access is controlled and monitored via a DD2875, access reviews are conducted no less than annually.

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	29
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	107
[ ]	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:	10/13/2020
[ ]	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.

ATO extended until May 12, 2021.

(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 007-97-01-01-02-8196-00 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	Stephanie Paschel	(1) Title	System Manager
(2) Organization	ZTCA	(3) Work Telephone	216.204.3029
(4) DSN		(5) E-mail address	stephanie.k.paschel.civ@mail.mil
(6) Date of Review	4/29/2020	(7) Signature	PASCHEL.STEPHANIE.K.1266457690 Digitally signed by PASCHEL.STEPHANIE.K.1266457690 Date: 2020.04.29 07:26:11 -04'00'
b. Other Official *(to be used at Component discretion)*	Kristina Krebs	(1) Title	Director IT Accounting Services
(2) Organization	ZTC	(3) Work Telephone	216.204.3327
(4) DSN		(5) E-mail address	kristina.l.krebs.civ@mail.mil
(6) Date of Review	05/06/20	(7) Signature	KREBS.KRISTINA.L.1251897170 Digitally signed by KREBS.KRISTINA.L.1251897170 Date: 2020.05.06 13:40:59 -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-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	07/17/20	(7) Signature	OUTLAW.GREGORY.L.1085047317 Digitally signed by OUTLAW.GREGORY.L.1085047317 Date: 2020.07.17 11:08:28 -04'00'

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	07/17/20	(7) Signature	MULLINS.RALPH.EDWARD.JR.1059546534 Digitally signed by MULLINS.RALPH.EDWARD.JR.1059546534 Date: 2020.07.17 11:20:53 -04'00'
f. Component Senior Information Security Officer or Designee Name	Jack Schiller	(1) Title	Deputy 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:	11/10/20	(7) Signature	SCHILLER.JACK.JOSEPH.1457280200 Digitally signed by SCHILLER.JACK.JOSEPH.1457280200 Date: 2020.11.18 15:36:56 -05'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name	Angela 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	07/22/20	(7) Signature	SCHULTZ.ANGELA.RENAE.E.1230338309 SCHULTZ.ANGELA.RENAE.E.1230338309 2020.07.22 10:02:06 -04'00'
h. Component CIO Reviewing Official Name	G. Paul Gass	(1) Title	Director, Information Technology
(2) Organization	DFAS-ZT	(3) Work Telephone	317.212.1161
(4) DSN	699.4800	(5) E-mail address	gregory.p.gass2.civ@mail.mil
(6) Date of Review	11/23/20	(7) Signature	GASS.GREGORY.PAUL.II.1109700440 2020.11.23 12:37:05 -05'00'

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.