

# 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:**

Computerized Accounts Payable System - Windows (CAPS-W)

**2. DOD COMPONENT NAME:**

Defense Finance and Accounting Service

**3. PIA APPROVAL DATE:**

03/18/20

## 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.**

CAPS-W automates the entitlement process associated with vendor pay operations within the Accounts Payable organizations. Each site processes vendor payments for different customers to include the United States Army, Marine Corps, and Defense Agencies. Accounts Payable organizations ensure entitlements are authorized, processed, validated, certified, and monitored for any errors in processing, both systemically and manually. CAPS-W looks for a three-way match (purchase order/invoice/receiving report) to calculate entitlements. The system also facilitates compliance with the Prompt Payment Act (PPA) to reduce interest penalty payments, discounts lost, and time spent in processing payment. Types of personal information contained within the system include vendor information such as: Social Security Number (SSN)/Tax Identification Number (TIN), address, DoD-ID, and Electronic Funds Transfer (EFT) financial payment information.

**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 PII is collected in order to support the vendor payment process.

**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.

CAPS-W source information is from interfaces with other systems. There is no PII collected from individuals.

**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.

CAPS-W source information is from interfaces with other systems. There is no PII collected from individuals.

**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

**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.
- 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.
- 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
- Existing DoD Information Systems  Commercial Systems
- Other Federal Information Systems

Standard Procurement System, Wide Area Workflow, Third Party Payment System-Transportation, Defense Travel System, Government Purchase Card, and Simplified Non-Standard Item Acquisition Program

**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
- Information Sharing - System to System  Website/E-Form
- Other (If Other, enter the information in the box below)

**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

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

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

(3) Retention Instructions.

Cutoff at the end of the fiscal year and destroy 10 years after 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 statute 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.

Department Regulations, Department of Defense Financial Management Regulation (DoDFMR), 7000.14R, Vol. 10; 31 U.S.C Sections 3512 and 3513; and E.O. 9397 Social Security Number (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 collect PII directly from individuals therefore it does not require an OMB approval number.

**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)

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

Other ID Number - Tax Identification Numbers

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.

SSN Justification Memorandum is in the process of being updated.

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

The Department of Defense Instruction 1000.30, enclosure 2, paragraph 2.c.(7) "Federal Taxpayer Identification Number".

(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".

SSNs and other key identifiers to tie to individuals are masked.

(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

The SSN is necessary to support tax reporting procedures.

**b. What is the PII confidentiality impact level<sup>2</sup>?**  Low  Moderate  High

<sup>1</sup>The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

<sup>2</sup>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)*

- |   |  |
|---|--|
| <input type="checkbox"/> Cipher Locks                 | <input checked="" type="checkbox"/> Closed Circuit TV (CCTV)                         |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges                            |
| <input checked="" type="checkbox"/> Key Cards         | <input type="checkbox"/> Safes   |
| <input checked="" type="checkbox"/> Security Guards   | <input checked="" type="checkbox"/> If Other, enter the information in the box below |

The PII will be secured by the physical controls indicated above. CAPS-W inherits all physical controls for protecting PII information from the DFAS Enterprise Local Area Network (ELAN).

(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

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

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

**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<sup>3</sup>?**

<input checked="" type="checkbox"/> Yes, DITPR	DITPR System Identification Number	<input type="text" value="3115"/>
<input type="checkbox"/> Yes, SIPRNET	SIPRNET Identification Number	<input type="text"/>
<input checked="" type="checkbox"/> Yes, RMF tool	RMF tool Identification Number	<input type="text" value="88"/>
<input type="checkbox"/> 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:

<input checked="" type="checkbox"/> Authorization to Operate (ATO)	Date Granted:	<input type="text" value="7/15/2017"/>
<input type="checkbox"/> ATO with Conditions	Date Granted:	<input type="text"/>
<input type="checkbox"/> Denial of Authorization to Operate (DATO)	Date Granted:	<input type="text"/>
<input type="checkbox"/> Interim Authorization to Test (IATT)	Date Granted:	<input type="text"/>

(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  If unsure, consult the component IT Budget Point of Contact to obtain the UII

<sup>3</sup>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.

<b>a. Program Manager or Designee Name</b>	Brian A. Smith	(1) Title	System Manager	
	(2) Organization	DFAS-IN/ZTCAD	(3) Work Telephone	317-212-5462
	(4) DSN		(5) E-mail address	brian.a.smith250.civ@mail.mil
	(6) Date of Review	12/10/19	(7) Signature	
<b>b. Other Official (to be used at Component discretion)</b>	Sally McManus	(1) Title	System Director	
	(2) Organization	ZTC Accounting Services	(3) Work Telephone	317-212-6751
	(4) DSN	699-6751	(5) E-mail address	sally.m.mcmanus.civ@mail.mil
	(6) Date of Review	02/07/20	(7) Signature	
<b>c. Other Official (to be used at Component discretion)</b>		(1) Title		
	(2) Organization		(3) Work Telephone	
	(4) DSN		(5) E-mail address	
	(6) Date of Review		(7) Signature	
<b>d. Component Privacy Officer (CPO)</b>	Gregory L. Outlaw	(1) Title	Privacy Program Manager	
	(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	02/20/20	(7) Signature	

<b>e. Component Records Officer</b>	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	02/20/20	(7) Signature	
<b>f. Component Senior Information Security Officer or Designee Name</b>	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:	03/12/20	(7) Signature	
<b>g. Senior Component Official for Privacy (SCOP) or Designee Name</b>	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	
<b>h. Component CIO Reviewing Official Name</b>	G. Paul Gass	(1) Title	Director, Information and 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	03/13/20	(7) Signature	

**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.mil](mailto:osd.mc-alex.dod-cio.mbx.pia@mail.mil).

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.