PRIVACY IMPACT ASSESSMENT (PIA)

For the

Wide Area Workflow (WAWF)
Business Transformation Agency (BTA)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	New DoD Information System	☐	New Electronic Collection
☐	Existing DoD Information System	☐	Existing Electronic Collection
☒	Significantly Modified DoD Information System		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	Yes, DITPR	Enter DITPR System Identification Number	432
☐	Yes, SIPRNET	Enter SIPRNET Identification Number	
☐	No		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ Yes ☐ No

If "Yes," enter UPI: 007-97-01-29-02-6577-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

☒ Yes ☐ No

If "Yes," enter Privacy Act SORN Identifier: Pending Development

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number	Chris Forshey will locate OMB Control Number.
Enter Expiration Date	

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

5 United States Code (U.S.C.), Section 301; Departmental Regulations; 10 U.S.C Sections 2733, 2734, 2734a, 2734b, 2735, 2736, 2737, 2738; 37 U.S.C, Section 404, Travel and transportation allowances: general; Department of Defense Directive 5154.29, Department of Defense Pay and Allowances Policy and Procedures; Department of Defense Financial Management Regulation 7000.14-R, Volume 9.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Wide Area Workflow (WAWF) provides the Department and its suppliers the single point of entry to generate, capture, and process invoice, acceptance, and payments related documentation and data to support the Department of Defense (DoD) asset visibility, tracking, and payment process. It provides the nexus of information related to acceptance of goods and services in support of the DoD supply chain.

Miscellaneous Payment Transaction processing can begin as a paper-based collection but information is transcribed from several different paper forms into a web-based data capture directly in WAWF or via Secure File Transfer protocol (SFTP) communicated to WAWF.

Individual's name, Social Security Number (SSN), Banking Account Number, Bank Routing Number, Bank Account Type (i.e. Checking/Savings), Home Address, City, State, Zip, Personal E-mail Address, and Home Telephone Number is collected. Information is entered by a government employee on behalf of the military, civilian, or federal retiree claimant.

Future implementation plan is to retrieve Banking Account Number, Bank Routing Number, Bank Account Type, Home Address, City, State, and Zip will be retrieved from Certified Electronic Funds Transfer (CEFT) for only military, civilian, and federal retiree. In unique cases, the same information will be collected from non-military, non-civilian persons.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The first privacy risk is with Access to Personally Identifiable Information (PII). Access to WAWF is controlled via Common Access Card (CAC) with PKI encryption or Software Certificate limited to individuals who are properly screened and cleared on a role based/need to know basis in the performance of their duties. Access to WAWF application is accessed through a protected .mil domain web address using Secure Socket Layer (SSL). Procedures are in place to deter and detect browsing and unauthorized access.

The second privacy risk is Unmasked PII: Currently, WAWF masks the SSN upon retrieval of data. In addition, the Tax Payer Identification Number (TIN), Banking Account, Bank Routing, and type of account information are encrypted in the database and application code.

The third risk would be Protection of PII: WAWF encrypts using FIPS 140-2 DoD compliant encryption (DBMS Crypto) method for data at rest and in transit. The data at rest are encrypted and located on servers at DISA DECC Ogden and protected by several layers of security and continuous monitoring. Privileged users are trained annually in accordance with DoD policies and procedures.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. All authorized WAWF users within the BTA.

☒ **Other DoD Components.**

Specify. The information is entered into any one of the DFAS entitlement systems such as Mechanization of Contract Administration Services (MOCAS), ONE-PAY, Integrated Accounts Payable System (IAPS), Standard Automated Material Management System (SAMMS), Computerized Accounts Payable System (CAPS), and Business Systems Modernization (BSM). The DFAS 'Blanket Routine Uses' apply to these systems (http://www.defenselink.mil/privacy/notices/dfas/dfas_preamble.html).

☒ **Other Federal Agencies.**

Specify. These systems may share this information with the Internal Revenue Service to report taxable earnings and taxes withheld, accounting, and tax audits, and to compute or resolve tax liability. Federal Reserve banks to distribute payments made through the direct deposit system to financial organizations or their processing agents authorized by individuals to receive and deposit payments in their accounts.

☒ **State and Local Agencies.**

Specify. Any information normally contained in Internal Revenue Service (IRS) Form W 2 which is maintained in a record from a system of records maintained by a Component may be disclosed to State and local taxing authorities with which the Secretary of the Treasury has entered into agreements under sections 5516, 5517, 5520 of 5 U.S.C., and only to those State and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Fiscal Requirements Manual Bulletin No. 76 07.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. The language in the contract for WAWF Program Management Office (PMO) Contractors to safeguards Personally Identifiable Information is listed below:

Section 5.1.4 Security and Privacy

DoD 5200.2-R, DoD Personnel Security Program, requires DoD military and civilian personnel, as well as DoD consultant and contractor personnel, who perform work on sensitive automated information systems (ISs), to be assigned to positions which are designated at one of two sensitivity levels (IT-I, IT-II). These designations equate to Critical Sensitive, Non-critical Sensitive. The contractor will assure that individuals assigned to the following sensitive positions, as determined by the Government, have completed the appropriate forms.

The required investigation will be completed prior to the assignment of individuals to sensitive duties associated with the position. The contractor will forward their employee clearance information (completed SF 85P, Questionnaire for Positions of Public Trust, and two DD Forms 258 (Fingerprint cards) to: DISA Security Division (MPS6); ATTN: Personnel Security (MPS62); P.O Box 4502, Arlington, VA 22204-4502.

DISA retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this contract, clearly conflict with the interests of the Government. The reason for removal will be fully documented in writing by the Contracting Officer. When and if such removal occurs, the contractor will within 30 working days assign qualified personnel to any vacancy(ies) thus created.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Every Department of Defense (DD) form for requesting reimbursement has a privacy act statement. Disclosure of the SSN and other requested information is voluntary; however, failure to provide the information necessary required to support the claim may result in delay or inability to process a claim for reimbursement.

(2) If "No," state the reason why individuals cannot object.

j. 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.

The Privacy Act Statements disclosing the use of their PII are provided to the individual when the individual submits a claim.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. **What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

When an individual is claiming reimbursement for a claim, a Privacy Act Statement is provided.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.