September 22, 2017

PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Workload Operations Web System (DWOWS)
Defense Finance and Accounting Service

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

☐ **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

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 T7340C

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

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 U.S. Code Chapter 55, Pay Administration; 37 U.S. Code Chapter 19, Pay and Allowance of the Uniformed Services; Department of Defense Financial Management Regulation (DoDFMR) 7000.14-R, Vol 7A; and E.O. 9397 Social Security Number as amended .E.O. 9397 Social Security Number as amended.

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.

DWOWS is a web-based system used by DFAS to track communications and inquiries (e-mail, faxes, letters, memorandum and phone calls) received and processed for Marine Corps and Navy Active Duty and Reserve members in resolving and reporting on military pay cases. It is used by management for benchmark reporting in order to track the turn-around time on financial inquiries.

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

Although there may be a potential risk to a system which collects personal identifiable information, DWOWS has taken measures to mitigate the risk.
-Access to the facilities is restricted to authorized DoD employees and contractors.
-Managed firewalls prevent access by other systems or network traffic not specifically identified in the firewall rule base.
-Access controls limit access to the application and/or specific functional areas of the application. Individuals are granted access to the system only after they have been verified to have a defined need to have access to the information and have gone through background and employment investigations, and are required to take yearly Information Assurance training and Spirit Training. Users are given only those system privileges based on their need to know and which are necessary for their job requirements.
-A Risk Management Framework assessment was completed for DWOWS in accordance with the requirements of the Federal Information Security Act of 2002 (FISMA) to audit policies, procedures, controls, and contingency planning, a requirement for all federal government information technology systems. DFAS adheres to physical protections of personal identifiable information as described in accordance with DFAS 5200.1-R. Information Assurance Policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include personal identifiable information, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8510.01.

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. Internal DFAS organizations affiliated with Military Pay Operations, that demonstrate a 'need to know,' and who are authorized to work on case management in the DWOWS system, will have access to PII data contained within the DWOWS system.

☒ **Other DoD Components.**

Specify. DWOWS provides case management for the Navy. Individuals from the Navy organizations listed below that demonstrate a 'need to know,' and who are authorized to work on case management in the DWOWS system, will have access to PII data contained within the DWOWS system.
Navy organizations:
Navy Personnel Command (NPC), Navy Personnel Support Detachments

(PSDs), Navy Afloat Activities (Fleet or Ships), U.S. Naval Academy, and the Naval Postgraduate School.

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. N/A

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

Specify. N/A

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.

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

DWOWS does NOT collect PII directly from the individual.

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.

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

DWOWS does NOT collect PII directly from the individual.

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.

DWOWS does NOT collect PII directly from the individual.

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.