PRIVACY IMPACT ASSESSMENT (PIA)

For the

Transaction Online Processing System (TOPS) Afloat
DEPARTMENT OF THE NAVY - CNIC

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	TWMS: DITPR: 6976 DITPR DON: 21023
☐	**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 TWMS UII: 007-000001569

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 TWMS SORN: N05230-1

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.

Authorities;

10 U.S.C 5013, Secretary of the Navy
10 U.S.C. 5041 Headquarters, Marine Corps
CNICINST 5230.1, Total Workforce Management Services
OPNAVINST 3440.17, Navy Installations Emergency Management Program
E.O. 9397 (SSN), 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.

The Transaction Online Processing System (TOPS) Afloat is a web based application designed for the Navy Information Application Product Suite (NIAPS). As such, it resides within NIAPS, which has a DITPR-DON # of 20955.

TOPS Afloat allows NIAPS users to initiate transactions within TOPS, which is a tool within the Total Workforce Management Services (TWMS) system (DITPR DON # 21023). TOPS is a web based interface to a SQL Server database and a file repository. It provides a method for the secure and rapid transmission of pay and personnel information between customers and Personnel Support Centers, while ensuring that appropriate safeguards are met for all Personally Identifiable Information under the Privacy Act.

TOPS Afloat is a customized version of TOPS which contains only the functionality needed to create transactions and upload files in support of those transactions. All data and file uploads generated by TOPS Afloat are then imported into TWMS on a regular basis. Technical Account management for the TOPS tool is managed solely by TWMS, and access to TOPS Afloat is determined by the user's existing access to the TOPS tool in TWMS.

Tracked PII is limited to Employee names and social security numbers along with scanned forms and documents relating to Navy Pay & Personnel functions.

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

Risks include unauthorized disclosure by personnel with access, and network intrusion. Access to the software is limited to those with a valid User ID and password. User IDs and passwords are managed within TWMS, which means that user accounts cannot be created or modified by TOPS Afloat.

Unauthorized disclosure is mitigated by limiting the scope of the data a user can access once logged in. Each account can only access transactions initiated by their same ship. They can only see 'Pending' transactions, and they cannot see file uploads associated with the transaction. File uploads are not accessible for download with the TOPS Afloat application. Once uploaded, the files can only be downloaded through TWMS.

Physical Intrusion is mitigated by the encryption of both the data field containing the SSNs, as well as the encryption of all uploaded files.

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. TWMS, Navy Information Application Product Suite (NIAPS)

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify.

☐ **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.

Individuals can object to the collection of PII by declining to provide the information unless specified as mandatory for "key", "emergency", or "critical" essential personnel as designated in OPNAVINST 3440.17.

Information is provided directly from the individual or their Command PASS Coordinator. Information collected is only that which is necessary to perform the associated Navy pay & Personnel Support Center (NPPSC) function. Individuals are free to object to the collection, however, this may impact NPPSC's ability to support them.

(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.

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

The individual initiates the transaction thereby consenting to the use of their personal information.

Information is provided directly from the individual or their Command PASS Coordinator. Information collected is only that which is necessary to perform the associated Navy pay & Personnel Support Center (NPPSC) function. Individuals are free to object to the collection, however, this may impact NPPSC's ability to support them.

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.

The TOPS Afloat log in page contains a Privacy Advisory that informs the user of the authority, purpose, and routine uses for the collection of PII.

Statement reads:

PRIVACY ACT SENSITIVE MATERIALS CONTAINED WITHIN
Any misuse or unauthorized disclosure of this information may result in both civil and criminal penalties.
When accessing and/or printing Personal Identity Information (PII), safeguard all information and documents. Misuse or mishandling of such information is prohibited in accordance with the Privacy Act of 1974.

PRIVACE ACT STATEMENT
You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you are consenting to the following conditions:

*The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
* At any time, the USG may inspect and seize data stored on this IS.
* Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
* This IS includes security measures (e.g., authentication and access controls) to protect USG interests -- not for your personal benefit or privacy.
* Notwithstanding the above, using this IS does not constitute consent to PE, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.
TOPS is a module of the Total Workforce Management Services (TWMS).

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.