PRIVACY IMPACT ASSESSMENT (PIA)

For the

Peoplesoft Officer Promotion Administrative System (PSOPAS)
US Navy

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	DITPR DON ID: 22133; DADMS ID: 31768
□	**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 PB2010: 007-17-01-20-02-4059-00

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 N01070-3; Navy Military Personnel Records System (System rec

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.

Title 10 U.S.C 5013, Secretary of the Navy (The Secretary of the Navy is responsible for...all affairs of the Department of the Navy, including....Administering (including the morale and welfare of personnel) and the Secretary is also responsible for such other activities as may be prescribed by the President or Secretary of Defense; see 10 U.S.C. (Armed Forces), Sections 611 (Convening of Selection Boards), 612, 620, 640, 641, 14002, 14101, 14102 and 14002; Subtitle C, Navy and Marine Corps; DoD Instruction 1320.12 (Commissioned Officer Promotion Program); SECNAV Instruction 1420.1B (Promotion, Special Selection,Special Early Retirement, and Selective Early Removal Boards for Commissioned Officers of the Navy and Marine Corps).

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 PeopleSoft - Officer Promotion Administration System (PS-OPAS) maintains officer personnel data applicable to the promotion and selection board process. It also supports creating files for the selection boards, loading board results, and processing of the monthly promotion process. It maintains a promotion history for all officers.

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

The following describes the various types of threats to PS OPAS privacy data, their associated potential impact, and the actions taken by the NSIPS architecture to mitigate those risks:

Risk: Unauthorized access to PS OPAS data in transit, addressed by implemented encryption and physical security.

Risk: Unauthorized access to PS OPAS data by authorized user, addressed by Authentication, policy, Network Architecture, active monitoring, role base access, and training

Risk: Unauthorized access to PS OPAS data by unauthorized user, addressed by all of the above plus encryption and physical security.

Risk: Residual data left in system's server or cache, addressed by security policy, encryption and physical security.

Risk: PS OPAS data is changed by authorized user, addressed by authentication, security policy, network encryption, active monitoring, physical security and role base access.

Risk: PS OPAS data is changed by unauthorized user, addressed by authentication, security policy, network encryption, active monitoring, physical security and role base access.

Risk: PS OPAS data is lost due to unauthorized user, addressed by authentication, security policy, active monitoring, physical security and role base access.

Risk: PS OPAS loss of availability, addressed by security policy, network architecture, active monitoring, physical security, training.

Risk: Middleware, addressed by authentication, security policy, encryption, active monitoring.

Risk: Social Engineering, addressed by authentication, security policy, physical security and training.

Risk: Client Security, addressed by security policy, encryption, network architecture, and training.

Risk: Promotion Data, addressed by authentication, security policy, network architecture, encryption, active monitoring, physical security, role base access and training.

Risk: Administrator Error, addressed by security policy, active monitoring, role base access and training.

The risks describes above are mitigated and data is safeguarded by the use of the following security countermeasures:

Threats Authentication Policy, Encryption Network Architecture, Active Monitoring, Physical Security, Role Based Access, and mandatory IA Training.

In addition All PSOPAS interfaces (data flow) are documented in either an ICD or MOA and are part of the SSAA. The PSOPAS system adheres to DON Security Policy.

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.
BUPERS N1: Officer Personnel Information System (OPINS)
BUPERS N1: Inactive Manpower Personnel Management Information System (IMAPMIS)
BUPERS N1: Navy Personnel Database (NPDB)

□ **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.

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

Data is necessary to conduct Navy Officer promotion boards.

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 data in PSOPAS is required to manage the military member's promotion records. Data is restricted to those individuals participating in the promotion board process.

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.

Individuals are not asked to provide personal data specifically for PS OPAS. However, officer promotion board information is gathered from other BUPERS/N1 systems that do provide a Privacy Act Statement regarding personal information requested for use in the database supported by the PS-OPAS IT system. The other systems are: Officer Personnel Information System (OPINS), Inactive Manpower Personnel Management Information System (IMAPMIS), Navy Personnel Database (NPDB). These SORN cited for these systems cite 10 U.S.C. 5013 as authority, N01070-3.

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.