



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Officer Personnel Planning System (OCMBLD Application) (NOPPS II - OCM)

Department of the Navy - BUPERS

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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

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

NOPPS II - OCM does not collect information from members of the public.

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.

SORN N01080-2, Officer Master File Automated Systems (November 01, 2013, 78 FR 65620),
authorities:

10 U.S.C. 5013, Secretary of the Navy and E.O. 9397 (SSN).

Other authorities:

U.S Code Title 10 Armed Forces
Subtitle C - Navy and Marine Corps (Vol II: 1835)
Part II: Personnel

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.

NOPPS II is designed to capture official strength activity to be used for certifying congressional compliance, budgeting, and creating the Five Year Defense Plan (FYDP). The program is sponsored by the Strategic Resourcing Branch (N100). NOPPS II is comprised of three main subsystems: Budget, Funds Administration, and Managerial Analysis. The Extract uses as input the official monthly cuts of the Officer Master File from OPINS II. It compares two successive month-end files and collects all changes of interest between the two files. Changes of interest are those affecting Military Personnel, Navy (MPN) strength or those related to promotions, movement, education, etc. of MPN strength. The changes are characterized as Gain, Loss, Designator Change, and Grade Change or informational. The Inventory Data Base module is used to prepare data for update, build the Inventory Data Base and query the Inventory Data Base. There are two components to this module. The Data Preparation module prepares the data for update and spins off a file to be used by NPRST for input to the OPIS/Highlander system. The main function of this module is to assign Strength Categories to each transaction/change. The Update and Search module is used to update the Inventory Data Base and to perform ad-hoc and canned queries of the database. Excel Pivots of strength activity are also built for distribution to officer community managers (OCMs).

PII collected: Name, SSN, rank, gender, race/ethnicity, birth date, military record: rank, designator, date of service, date of rank

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

The collection of personal information presents a risk because of the potentially sensitive nature of the information and the consequence of the data being mishandled, which could lead to unwarranted invasion of the individual's privacy. This risk is mitigated by ensuring that access to the data is strictly controlled and by making sure that all administrative, technical, and physical controls are in place to protect the data.

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.

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.

Contracting Company: SAG Corporation

Contractors must sign a Non-Disclosure Agreement to assure confidentiality and also complete yearly DOD Information Assurance Training.

The Contractor agrees to:

(1) The Contractor will be required to design, develop, or operate a system of record on individuals, to accomplish an agency function subject to the Privacy Act of 1974 (the Act) and applicable agency regulations when the contract specifically identifies:

(i) the system of record; and

(ii) The design, development, operation work that the contractor is to perform
(2) Include the Privacy Act Notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work in the proposed subcontract requires the design, development, or operation of a system of record on individuals that is subject to the Act.

• Keep government furnished laptop in a secure government space or under lock and key when not in use.

• Laptops have full disk /data at rest (DAR) encryption using a DoD/DON approved DAR solution.

• Not to store PII on personal electronic storage devices.

The SAG Corporation does not contain the required FAR privacy clauses. They will be added in the next contract mod.

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.

Information is not collected 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.

Information is not collected 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

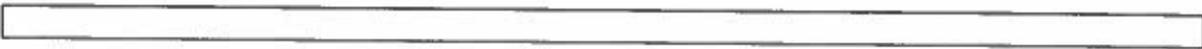
Privacy Advisory

Other

None

Describe each applicable format.

Information is not collected 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.