



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Electronic Military Personnel Records System (EMPRS)

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 DITPR ID: 109 DITPR DON ID: 10285
- 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

UJI: 007-000000737

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

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

EMPRS does not collect personal information from the general 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 authorities:

10 U.S.C. 5013, Secretary of the Navy
42 U.S.C. 10606 as implemented by DoD Instruction 1030.1, Victim and Witness Assistance Procedures E.O. 9397 (SSN), as amended.

Other authorities:

44 USC 3101, Records Management by Agency Heads
5 U.S.C. 552a, Records Maintained on Individuals
36 CFR 1220, Federal Records; E.O. 9397 (SSN)
DODI 1336.08, Military Human Resource Records Life Cycle Management
BUPERSINST 1070.27C, Document Submission Guidelines for the Electronic Military Personnel Records System

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.

EMPRS is an approved electronics records management application established to provide electronic document management of the Official Military Personnel File (OMPF) for each officer and enlisted member of the Navy, from the time of entry into the service until ownership of the record is transferred to the National Archives 62 years after completion of a service member's obligated service. The OMPF consists of data and images of standard military human resource documents required by DoD and DON which are used to support life-cycle management of a Sailor; applicable to events related to a military member's career and/or protect the legal and financial rights of the Government and of persons directly affected by the agency's activities; and data and documents relating to a request for access to an individual record, letters of denial, appeals, and related documents and audit data collected through the "OMPF My Record", "OMPF Command View", and "Request Record on CD" applications which is accumulated in processing requests received under the Privacy Act of 1974, as amended.

Types of information collected in this system consists of individual's name and other names used, Social Security Number (SSN) (both full and truncated), driver's license, DoD ID number, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, personal cell telephone number, home telephone number, personal email address, mailing/home address, religious preference, security clearance, mother's maiden name, mother's middle name, marital status, emergency contact, spouse and child information: to support dependency determination which are used to entitlements and benefits such as name, relationship, gender, date of marriage, home/ mailing address, home/mobile phone number, date of birth, and designation of beneficiaries in case a member becomes a casualty; medical information: accession and separation physical examination documentation is collected, in addition to results of medical boards; enlistment service number, office file number, rank/rate, designator, military status, military records: correspondence and records in both automated and non-automated form containing accession information, classification, assignments, promotion, advancements, performance, decorations and awards, reenlistment and extension information, separation and retirement related information, training, education, personal affairs, casualty documentation, benefits, entitlements, discipline-related information, entry and separation physical examinations, and personal documents and non-service related documents deemed necessary and appropriate for the administration of naval personnel; education information: includes highest grade completed, and degrees received from accredited colleges, and military training courses; disability information: type of disability and bometrics information: fingerprints, body markings, and DNA sample.

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

Inadvertent exposure of PII as a result of user mistake, mitigated by restricting access to the production area where paper documents and images are being processed; having multiple layers of quality control to preclude misfiled documents; and manual reviews of all documents or records distributed to preclude distribution of documents to unauthorized personnel.

Attacks or intrusion into EMPRS by unauthorized personnel; mitigated through the use of PKI, firewall, restricted access to files based on user permissions.

Copy of OMPF CD-ROM falling into unauthorized person's possession; mitigated through the use of a AES 128 bit encryption of the CD-ROM files, coupled with password activation method.

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. **Individuals/service members, Commanders and other Navy staff principals in**

the chain of command, U.S. Navy Recruiting Command, Human Resources managers and clerical staff servicing the individual Sailors, the Navy Inspector General offices, Navy Financial Management and Audit organizations, Navy Criminal Investigation Service (NCIS), and Selection Boards, the Navy Judge Advocate General and servicing Navy legal offices.

Other DoD Components.

Specify. The Office of the Under Secretary of Defense for Personnel and Readiness, Personnel and Readiness Information Management; Defense Finance and Accounting Service; Defense Intelligence Agency; Defense Criminal Investigative Service; DoD Inspector General; the U.S. Air Force; the U.S. Army; the U.S. Marine Corps; and other DoD organizations on an individual basis with a need to know.

Other Federal Agencies.

Specify. The National Archives and Records Administration (NARA); The Department of Veterans Affairs (VA); the Office of Personnel Management (OPM); the Department of Homeland Security; the Federal Bureau of Investigation (FBI), the State Department; the Treasury Department; the Department of Labor; the Department of Justice; the U.S. Coast Guard; the Social Security Administration; Department of Health and Human Services; and the President of the U.S.

State and Local Agencies.

Specify. Law enforcement agencies; various state and local agencies performing duties related to verification of status for determination of eligibility for benefits and entitlements.

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

Specify. Leidos, Data Networks Corporation (DNC), and SAIC. The required privacy clauses are included in each contract.

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

Specify. National Research Council; Navy Relief and American Red Cross; private organizations under government contract

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.

PII provided by the individual is used to support the life-cycle management of the sailor's/military member's career.

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.

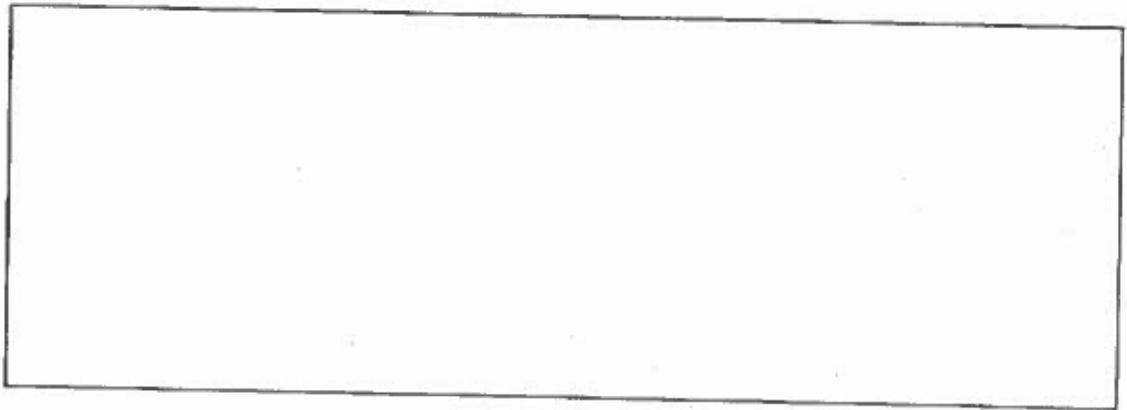
PII provided by the individual is used to support the life-cycle management of the sailor's/military member's career.

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.

Required FOUO and Privacy Act disclaimers are displayed throughout the site; the DOD required Privacy and Monitoring Advisory is provided at login; and a Privacy Act Statement is provided to the individual by a Human Resources Specialist prior to collection of PII from the sailor.



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.

