



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Inactive Manpower and Personnel Management Information System (IMAPMIS)

SPAWAR - 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
- 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

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 and E.O. 9397 (SSN)

Navy Military Personnel Manual (MILPERSMAN) --NAVPERS 15560D

DoD Records Management Program, SECNAV M-5210.1, December 2005.

Title 5 U.S.C. 301, Departmental Regulations (Cited as authority in SORN N01080-3); Title 10 U.S.C. 5013, Secretary of the Navy; SECNAVINST 5312.10C (Issued by the Secretary of the Navy: Manpower Planning Systems); and OPNAVINST 1000.16J (Manual of Navy Total Force Manpower Policies and Procedures, Implementing SECNAVINST 5312.10C).

5 U.S.C. 301--Authorizes a military department to prescribe regulations for the government of his department. 10 U.S.C. 5013 Authorizes the Secretary of the Navy, as the department head of the Navy, to do what is necessary to conduct all affairs of the Department of the Navy, including assignment, detail and duties of its members. SECNAVINST 5312.10C and OPNAVINST 1000.16J carry out that responsibility for management of the Navy's manpower. The IMAPMIS system functions to meet the Secretary's responsibilities to manage total force manpower, including the inactive manpower and 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.

IMAPMIS is the corporate database for the Navy's Inactive Reserve, maintaining 850,000 personnel master records for members of the Selected Reserve, Individual Ready Reserve (IRR), Standby Reserve, and all United States Navy (USN) and United States Navy Reserve (USNR) Retired. IMAPMIS supports IRR mobilization readiness and personnel data reporting. IMAPMIS accumulates participation information to determine Reserve members' eligibility for retirement and delivers Annual Retirement Point Records (ARPR) and Notices of Eligibility (NOE) to members via the Navy Web site.

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

PII data is stored on the IMAPMIS database on a Department of Defense Mainframe computer. The Defense Enterprise Computing Center (DECC) is responsible for operation of the mainframe. This system is protected by DON policy-compliant passwords, ACF2 access methods, encryption and fire walls to ensure only authorized personnel gain access to private information. The risk of data disclosure is very low. This system is protected by DON policy-compliant passwords, ACF2 access methods, encryption and firewalls to ensure only authorized personnel gain access to private information. Authorization to access the IMAPMIS database via online screens is the responsibility of the IMAPMIS Database Administrators. Specific procedures are also in force for the disposal of computer output. Output material in the sensitive category for which inadvertent or unauthorized disclosure that would result in harm, embarrassment, inconvenience or unfairness to the individual, will be shredded. IMAPMIS exchanges data with other Navy manpower systems, which reside in the same mainframe region. Due to these extensive procedures, the risk of data disclosure is very low. Data shared is maintained and controlled via MOU and ICD agreements. Data flows through DoN system to DoN system through secure channels. Authorization to access IMAPMIS data is the responsibility of the Navy Personnel Command (NPC), currently PERS341. Within the computer center, controls have been established to disseminate computer output over the counter only to authorized users. Specific procedures are also in force for the disposal of computer output. Output material in the sensitive category, i.e., inadvertent or unauthorized disclosure that would result in harm, embarrassment, inconvenience or unfairness to the individual, will be shredded. Computer files are kept in a secure, continuously manned area and are accessible only to authorized computer operators, programmers, enlisted management, placement, and distributing personnel who are directed to respond to valid, official request for data. These accesses are controlled and monitored by the security system.

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. Navy Bureau Of Medicine and Surgery (BUMED), Chief of Naval Education and Training (CNET), and Navy Manpower, Personnel, and Distribution Systems.

Other DoD Components.

Specify. Defense Manpower Data Center(DMDC), Defense Finance and Accounting Service (DFAS)

Other Federal Agencies.

Specify. Social Security Administration

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.

The Inactive Manpower and Personnel Management Information System, (IMAPMISS) is the corporate source for Inactive Duty Enlisted personnel data. This data is critical to manage the personnel records of Inactive Naval Personnel.

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 IMAPMIS is required to manage the military member's records.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|-----------------------------------------------------------|------------------------------------------------------|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

When Privacy Act information is requested of the service member, the individual is provided a Privacy Act Statement and Privacy Advisory.

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.