



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Bureau of Medicine (Navy) Manpower Information System II (BUMIS II)

Department of the Navy - TMA DHP Funded System - BUMED

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.

SORN Authorities:

5 U.S.C. 301, Departmental Regulations
10 CFR part 20, Standards for Protection Against Radiation
E.O. 9397 (SSN), as amended

Other Authorities:

OPNAVINST 1223.1B, "Navy Enlisted Occupational Classification System," August 13, 1993
OPNAVIST 1000.16J, "Manual of Navy Total Force Manpower Policies and Procedures," June 17, 2002
SECNAVINST 5312.10C, "Manpower Planning Systems," October 29, 1974

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.

BUMIS II provides an online inventory of personnel assigned to Navy Medicine. It includes demographics, education, health care specialty, additional qualifications, assignment and training skills. BUMIS II provides personnel planners at headquarters level with data about the medical personnel force that allows tracking and trends of gains, losses, and skill mix. The data is pivotal for the development of personnel strength plans, promotion plans, accession plans, and training plans and is also used for ad hoc queries responding to inquiries about medical department officer force from both inside and outside the Navy Medical department.

PII collected includes: name, birth date, Social Security Number (SSN), and military records to include rank, duty station, education and qualification and special pays data.

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

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that BUMIS II, with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

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.

Data is shared with individuals that have a need-to-know within the command. BUMIS II shares data with Interactive Manpower and Personnel Management System (IMAPMIS), Total Force Manpower Management System (TFMMS), Officer Personnel Information System (OPINS), Navy Enlisted Personnel System (NES), Naval Medical Education and Training Command (NMETC), and Dental Common Access System (DENCAS).

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.

General Dynamics Information Technology, Inc. The contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R, "DoD Privacy Program," May 14, 2007. The contractor shall also comply with federal laws relating to freedom of information and records management.

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.

PII for BUMIS II is not requested from and collected directly from the individual.

IAW SECNAVINST 5312.10C, "Manpower Planning Systems," October 29, 1974 and OPNAVIST 1000.16J, "Manual of Navy Total Force Manpower Policies and Procedures," June 17, 2002, the Chief of Naval Operations CNO directs and coordinates the development and implementation of the manpower planning system to plan, program and budget for total force manpower resources. Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSN's. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records.

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 for BUMIS II is not requested from and collected directly from the individual.

IAW SECNAVINST 5312.10C, "Manpower Planning Systems," October 29, 1974 and OPNAVIST 1000.16J, "Manual of Navy Total Force Manpower Policies and Procedures," June 17, 2002, the Chief of Naval Operations CNO directs and coordinates the development and implementation of the manpower planning system to plan, program and budget for total force manpower resources. Upon entrance into military service or civilian employment with the Department of Defense, individuals are asked to provide their SSN's. The SSN becomes the service or employment number for the individual and is used to establish personnel, financial, medical, and other official records.

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.

PII for BUMIS II is not requested from and 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.