



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Reserve Database Warehouse - Decision Support System (NRDW - DSS)
--

Department of the Navy - NAVRESFOR

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

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.

<p>SORN Authorities:</p> <p>5 U.S.C. 301, Department Regulations; DoD 6025.18-R, DoD Health Information Privacy Regulations; and E.O. 9397 (SSN), as amended</p> <p>Other Authorities:</p> <p>10 U.S.C. 5013, Department of the Navy 10 U.S.C. Subtitle E, Reserve Components 1007, Administration of Reserve Components BUPERS Instruction 1001.39F, Administration Procedures for Navy Personnel OPNAV Instruction 100.16K, Navy Total Force Manpower Policies and Procedures</p>

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.

Navy Reserve Database Warehouse-Decision Support System (NRDW-DSS) is a corporate data warehouse designed to effectively consolidate, integrate, and archive disparate Navy Reserve corporate legacy databases into a single, web-enabled, content rich information source. The system objective is to better inform leadership decision makers and to streamline data analysis efforts. It provides a foundation for Business Intelligence, provides projection and trend information for the entire Navy Reserve Force.

System to system interfaces with the Reserve Headquarters System (RHS), Navy Reserve Order Writing System (NROWS), Reserve Components Common Personnel Data System (RCCPDS), Navy Reserve Readiness Module (NRRM) and Navy Reserve Homeport (NRH) which provide the PII contained in NRDW-DSS.

NRDW-DSS stores records reflecting information pertaining to the individual's participation in the Reserves.

Personal information collected includes: Name, rank/grade, Social Security Number (SSN), citizenship, gender, race/ethnicity, date of birth, home telephone number, home mailing address, religious preference, security clearance, martial status, military records, Medical information includes: that information related to retention and advancement/promotion; Education Information includes: education level/major/speciality code, high school diploma or GED and years of education; and other pertinent information related to recruitment, classification, assignment, retention, reenlistment, promotion, advancement, training, education, professional history, experience, performance, qualifications, retirement, orders and administration Selected Reserves (SELRES).

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

The disclosure of the information stored in the NRDW-DSS could lead to identity theft/fraud or perhaps be used to target individuals for exploitation. The risks are mitigated via application security controls for user login, two-factor authentication via common access card (CAC), system monitoring by system administrators, policies and system security controls as outlined in the certification and accreditation (C&A) plan.

The data stored in the NRDW-DSS is protected by a variety of methods including data-at-rest/data-in-transit encryption, firewalls and intrusion detection systems (IDSs). Access to the data is restricted to authorized users only. All system users are required to undergo annual Privacy Act and Information Assurance (IA) training.

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.

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 is not solicited from the individual by NRDW-DSS. PII is collected by the authoritative source systems and securely transferred to NRDW - DSS on a periodic basis.

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 is not solicited from the individual by NRDW-DSS. PII is collected by the authoritative source systems and securely transferred to NRDW - DSS on a periodic basis. The individual's opportunity to consent would be at the collection point by the authoritative source systems. NRDW-DSS stores PII, but does not provide any mechanism for the collection of PII 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.

Serving as the Navy Reserve's data warehouse, NRDW-DSS stores data it receives via system to system interfaces with the various authoritative source systems. Individuals are never asked to provide PII to NRDW-DSS. The PII data contained in NRDW-DSS is supplied by authoritative source systems. The authoritative source systems collecting the PII has the responsibility of providing the individual with any information related to the collection of PII.

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.