PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Reserve Readiness Module (NRRM)
Department of the Navy - USFFC

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: DITPR ID: 4982 (DITPR DON ID: 20933)
- ☐ **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 007-000001335

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 N01080-3

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

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:

55 U.S.C. 301, Department Regulations
E.O. 9397 (SSN), as amended

Other authorities:

BUPERS INSTRUCTION 1001.39F, Administrative Procedures for Navy Reservists
OPNAV INSTRUCTION 1001.16K, Navy Total Force Manpower Policies and Procedures

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.

NRRM is a comprehensive data management system designed to consolidate, store, and manage readiness information for the U.S. Navy and Navy Reserves. This web-based program provides the capability for display and analysis of readiness data at various levels of detail to give the user a clear picture of current readiness of individuals and rolling up to units, regional and major command levels. NRRM is the primary readiness reporting system for the Navy Reserve.

PII is populated and updated by data sharing with MRRS, NMCMPS, NROWS, RHS, PRIMS and NTMPS. The individual does not provide PII nor do other users/administrators of the system.

PII collected by NRRM includes: Name, SSN (full and truncated), DoD ID number, gender, birth date, personal cell phone number, home phone number, personal email address, mailing/home address, security clearance, medical information, military records, education information, physical readiness results, special military qualifications (e.g., NEC, NOBC, etc.), training records, and future EDIPI identifier capability.

Rank is provided at account creation.

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, acts of nature (e.g., fire, flood), and improper data handling procedures. These risks threaten the availability of the system, the integrity and confidentiality of the data, and may lead to the misuse of information.

Mitigation Steps:
- User security roles: six user roles limit the visibility of personal information to those only with a need-to-know.
- Account control: military E7 and above with exceptions approved by the NRRM PM following endorsement by supervisor. Civilians require endorsement by military supervisor.

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 and Navy Reserve (e.g., Defense Readiness Reporting System - Navy)

☐ **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.

The PII data contained in the compiled readiness jacket for each individual is collected via secured periodic transfer from other DON systems to NRRM and does not involve the user's interaction or approval. If a person were to refuse to provide their rank at the point of account creation they would not be able to obtain an account.

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 PII data contained in the compiled readiness jacket for each individual is collected via secured periodic transfer from other DON systems to NRRM and does not involve the user's interaction or approval.

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.	The PII data contained in the compiled readiness jacket for each individual is collected via secured periodic transfer from other DON systems to NRRM and does not involve the user's interaction or approval.

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.