



PRIVACY IMPACT ASSESSMENT (PIA)

**Navy Readiness Reporting Enterprise (NRRE)
Department of the Navy**



**Reviewing Official
Chief Information Officer
United States Navy**

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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?

Navy Readiness Reporting Enterprise (NRRE)

- Yes, DITPR Enter DITPR System Identification Number
- Yes, SIPRNET Enter SIPRNET Identification Number
- No

Navy Readiness Reporting Enterprise (NRRE) (Continue)

DADMS ID Number Enter DADMS Identification Number

DITPR-DON ID Number Enter DITPR-DON Identification Number

Defense Readiness Reporting System – Navy (DRRS-N)

Yes, DITPR Enter DITPR System Identification Number

Yes, SIPRNET Enter SIPRNET Identification Number

No

Navy Global Force Management Organizational Server (Navy GFM Org Server)

Yes, DITPR Enter DITPR System Identification Number

Yes, SIPRNET Enter SIPRNET Identification Number

No

Note: Navy GFM Org Server is reflected as a component of DRRS-N.

TYCOM Readiness Management System (TRMS)

Yes, DITPR Enter DITPR System Identification Number

Yes, SIPRNET Enter SIPRNET Identification Number

No

Navy Training Information Management System (NTIMS)

Yes, DITPR Enter DITPR System Identification Number

Yes, SIPRNET Enter SIPRNET Identification Number

No

Navy Reserve Readiness Module (NRRM)

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?

Navy Readiness Reporting Enterprise (NRRE)

Yes **Enter UPI**
If unsure, consult the
Component IT Budget Point of Contact to obtain the UPI.

No

Defense Readiness Reporting System – Navy (DRRS-N)

Yes **Enter UPI**
If unsure, consult the
Component IT Budget Point of Contact to obtain the UPI.

No

Navy Global Force Management Organizational Server (Navy GFM Org Server)

Yes **Enter UPI**
If unsure, consult the
Component IT Budget Point of Contact to obtain the UPI.

No

Note: Navy GFM Org Server is reflected as a component of DRRS-N.

TYCOM Readiness Management System (TRMS)

Yes **Enter UPI**
If unsure, consult the
Component IT Budget Point of Contact to obtain the UPI.

No

Navy Training Information Management System (NTIMS)

Yes **Enter UPI**
If unsure, consult the
Component IT Budget Point of Contact to obtain the UPI.

No

Navy Reserve Readiness Module (NRRM)

Yes **Enter UPI**

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

No

d. Does the DoD information system or electronic collection have 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 **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.

No

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.

Defense Readiness Reporting System – Navy (DRRS-N)

Yes

Enter OMB Control Number

Enter Expiration Date

No

Navy Global Force Management Organizational Server (Navy GFM Org Server)

Yes

Enter OMB Control Number

Enter Expiration Date

No

TYCOM Readiness Management System (TRMS)

Yes

Enter OMB Control Number

Enter Expiration Date

No

Navy Training Information Management System (NTIMS)

Yes

Enter OMB Control Number

Enter Expiration Date

No

Navy Reserve Readiness Module (NRRM)

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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.

10 U.S.C 117, Readiness Reporting System: establishment
Reporting to Congressional Committees
10 U.S.C. 113, Secretary of Defense
DoD Directives 5149.2, Senior Readiness Oversight Council
DoD Directive 7730.65, Department of Defense Readiness Reporting System, and supplemental guidance
DoD Instruction 8260.03, Organizational and Force Structure Construct (OFSC) for Global Force Management (GFM).
Executive Order. 9397 (SSN).
Directive Type Memorandum (DTM) 07-015-USD (P&R), DoD Social Security Number (SSN) Reduction Plan, dated 28 Mar 08.
OPNAV Instruction 3501.360, Defense Readiness Reporting System - Navy (DRRS-N), dated 28 Jan 08.
BUPERS Instruction 1001.39F, Administrative Procedures for Navy Reservists
OPNAV Instruction 1000.16K, Navy Total Force Manpower Policies and Procedures
COMFLTFORCOM Instruction 3501.4, Defense Readiness Reporting System – Navy (DRRS-N) Reporting Manual, dated 08 Dec 08.

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.

The Navy Readiness Reporting Enterprise (NRRE) provides readiness data to the Defense Readiness Reporting System (DRRS),

The Navy Readiness Reporting Enterprise (NRRE) is an approach to capturing information and data necessary to manage Navy combat capabilities and resources and is part of a larger network, or Federation of Enterprises, that supports various Navy applications throughout the Department of the Navy. The NRRE is a compilation of these various Navy reporting and resource management applications that support the Navy's core mission through Readiness Reporting, Adaptive Planning, Force Sourcing, Force Management and Resource Tracking.

The NRRE collects information pertaining to readiness-related decision data that measures capability to accomplish assigned missions at all levels of the Navy. This data includes human resource status information; individual personnel readiness data to include name, employer, unit, rank/grade, duty status, deployability (individual medical readiness), skill specialty, and reason codes.

The information collected, including PII information will give the Navy Readiness Reporting Enterprise (NRRE) the ability to evaluate the overall readiness rather than simply reporting the data from multiple databases. This is accomplished by establishing a measurement of readiness through mission assessments by Department of Defense (DoD) components such as Combatant Commanders (CCDRs), Combat Support Agencies (CSAs), and Services. NRRE will permit commanders to obtain pertinent readiness data on personnel assigned/attached to their units.

Access to the Navy Readiness Reporting Enterprise (NRRE) is limited to authorized and appropriately cleared personnel as determined by the system manager. All Navy Readiness Reporting Enterprise (NRRE) information/records are maintained in controlled facilities. Physical entry is restricted by use of locks, guards, and is accessible only to authorized, cleared personnel. Access to information/records is limited to person(s) responsible for servicing analyzing the record in the performance of the official duties and who are properly screened and are cleared for the "need to know." Access to computerized data is restricted by passwords, which are required to be changed in accordance with current directives. Applications of the NRRE are stored on the Navy's NIPR and SIPR system.

The NRRE is a federation of Navy owned information systems that are comprised of:

- Defense Readiness Reporting System – Navy (DRRS-N)
- Navy Global Force Management Organizational Server (GFM Org)
- TYCOM Readiness Management System (TRMS)
- Navy Training Information Management System (NTIMS)
- Navy Reserve Readiness Module (NRRM)

Defense Readiness Reporting System – Navy (DRRS-N)

The Defense Readiness Reporting System Navy (DRRS-N) is the near real-time web-based tool used to assist Navy Commanders in performing readiness assessments and decision support for Mission Essential Task capability-based readiness reporting. The DRRS-N provides the unique ability to assess and report, via the chain-of-command, status of capabilities of any Navy unit, so that critical decisions can be made to deploy units in a timely manner based on accurate, up-to-date information.

Navy Global Force Management Organizational Server (Navy GFM Org Server)

The Navy Global Force Management (GFM) Organizational (GFM Org) server supports the transformational efforts of the GFM Data Initiative (GFM DI). The GFM DI establishes the ability to integrate organizational and force structure authorization data across the Department of Defense (DoD) enterprise and guides the development and implementation of the GFM Data Strategy to ensure organizational and force structure authorization data from the Office of the Secretary of Defense (OSD), the Joint Staff (JS), and the Services is integrated in a standardized manner. The GFM Org server exists in both NIPRNET and the SIPRNET domains. Minimum personal information is collected to establish and authenticate users on a need-to-know basis. The GFM Org server does not collect any other type of PII information.

TYCOM Readiness Management System (TRMS)

TYCOM Readiness Management System (TRMS) Ashore. TRMS is a world-view web-enabled readiness management system providing ad hoc data views, graphs and reports for AMMO, Schedule, SORTS, CASREP, ISIS, TRAREP and Personnel. TYCOM Readiness Management System (TRMS) Ashore.

Navy Training Information Management System (NTIMS)

The Navy Training Information Management System (NTIMS) is a fully web-enabled application that consists of an integrated suite of information management tools to identify, collect, analyze, store, and disseminate data required to execute Navy training and training readiness programs. NTIMS provides rapid operational analysis, planning, evaluation, and reporting of training events and requirements. It fully automates procedures, processes and information supporting service application of the Navy Warfare Training System (NWTS). NTIMS enables users to develop, plan, execute and assess Joint/Navy training to prepare war fighters, and those who support them, to meet service-wide standards performing assigned missions to the level required in accomplishing their assigned missions.

Navy Reserve Readiness Module (NRRM)

The Navy Reserve Readiness Module (NRRM) is a comprehensive data management system designed to consolidate, store, and manage readiness information for the Navy Reserves. NRRM is a web-based program and uses a two-tier architecture that consists of a web application and database servers which provide the capability for the display and analysis of readiness data at various levels of detail, providing the user with a clear picture of current readiness. NRRM is the primary readiness reporting system for the Navy Reserve to assess the training and mobilization of Reservists. NRRM provides users a macro view of basic Reserve organizational data to include deployed status, homeport, subordinate organizations, and parent organization.

The Navy Reserve Readiness Module (NRRM) has an approved Privacy Impact Assessment on file with the DON CIO. This Navy Reserve Readiness Module application is included in the Navy Readiness Reporting Enterprise Privacy Impact Assessment to accurately reflect its association in Navy Readiness Reporting.

(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, and acts of nature (e.g., fire, flood, etc.).

All systems are at risk because they may be vulnerable to unauthorized intrusion and hacking. There are risks that the Navy Readiness Reporting Enterprise (NRRE), with its collection of PII, could be comprised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

All systems are vulnerable to "insider threats." The NRRE System Managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access this information. There are defined criteria to identify who should have access to the NRRE. These individuals have gone through extensive background and employment checks.

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

OPNAV N1, USFFC N40

Other DoD Components. Specify

Office of the Secretary of Defense, Joint Staff, Defense Readiness Reporting System,

Other Federal Agencies. Specify

Various Congressional Offices and Departments
- Readiness Reports for the House Arm Services Committee.
- Readiness Reports for the Senate Arm Services Committee.

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

Center for Naval Analysis

i. Do individuals have the opportunity to object to the collection of their PII?

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

Defense Readiness Reporting System – Navy (DRRS-N)

Yes or **No**

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

DRRS–N application: PII data contained in the Defense Readiness Reporting System - Navy for mission related use and is provided by other systems. The DRRS–N application does not change or modify data from these authoritative data sources. Individuals would need to contact the System Managers for those source systems. These systems include:

Navy Standard Integrated Personnel System (NSIPS)
Enlisted Master File Automated Systems (EMFAS)
Medical Readiness Reporting System (MRRS)
Defense Civilian Personnel Data System (DCPDS)

Navy Global Force Management Organizational Server (Navy GFM Org Server)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

TYCOM Readiness Management System (TRMS)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

Navy Training Information Management System (NTIMS)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

Navy Reserve Readiness Module (NRRM)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

NRRM application: PII contained in the Navy Reserve Readiness Module is for mission related use and is provided by other systems. The NRRM application does not change or modify data from these authoritative data sources. Individuals would need to contact the System Managers for those source systems. These systems include:

Reserve Command Management Information
Medical Readiness Reporting System (MRRS)
Reserve Financial Management/Training System (RESFMS)
Physical Readiness Information Management System (PRIMS)
Navy Training Management and Planning System (NTMPS)

Navy-Marine Corps Mobilization Processing System (NMCMPMS)

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Defense Readiness Reporting System – Navy (DRRS-N)

Yes or **No**

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

DRRS–N application: PII data contained in the Defense Readiness Reporting System - Navy is for mission related use and is provided by other systems. The DRRS–N application does not change or modify data from these authoritative data sources. Individuals would need to contact the System Managers for those source systems. These systems include:

Navy Standard Integrated Personnel System (NSIPS)
Enlisted Master File Automated Systems (EMFAS)
Medical Readiness Reporting System (MRRS)
Defense Civilian Personnel Data System (DCPDS)

Navy Global Force Management Organizational Server (Navy GFM Org Server)

Yes or **No**

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

TYCOM Readiness Management System (TRMS)

Yes or **No**

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

Navy Training Information Management System (NTIMS)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

Navy Reserve Readiness Module (NRRM)

Yes or No

User Accounts: Individuals could elect not to provide PII when applying for access. Personnel requesting a user account are advised via hyperlink titled "Privacy Advisory" on that account request page that disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay, or prevent further processing of an account request. Users have the ability to update and correct their own personal information (User Profile).

NRRM application: PII contained in the Navy Reserve Readiness Module is for mission related use and is provided by other systems. The NRRM application does not change or modify data from these authoritative data sources. Individuals would need to contact the System Managers for those source systems. These systems include:

Reserve Command Management Information (RCMI)
Medical Readiness Reporting System (MRRS)
Reserve Financial Management/Training System (RESFMS)
Physical Readiness Information Management System (PRIMS)
Navy Training Management and Planning System (NTMPS)
Navy-Marine Corps Mobilization Processing System (NMCMPMS)

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

Defense Readiness Reporting System – Navy (DRRS-N)

“Privacy Act Notice” and “Privacy Advisory” pop-up screen

Navy Global Force, Management Organizational Server (Navy GFM Org Server)

“Privacy Act Notice” and “Privacy Advisory” pop-up screen

TYCOM Readiness Management System (TRMS)

“Privacy Act Notice” and “Privacy Advisory” pop-up screen

Navy Training Information Management System (NTIMS)

“Privacy Act Notice” and “Privacy Advisory” pop-up screen

Navy Reserve Readiness Module (NRRM)

“Privacy Act Notice” and “Privacy Advisory” pop-up screen

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.