



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Readiness and Cost Reporting Program (RCRP)

Department of the Navy - United States Fleet Forces Command

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.

SORN and additional authorities:

10 U.S.C. 5013, Secretary of the Navy

10 U.S.C. 117, Readiness Reporting System establishment: Reporting to Congressional Committees; Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3401.02B, 31 May 2011, Force Readiness Reporting

Department of Defense Directive 5124.02, 23 June 2008, Under Secretary of Defense for Personnel and Readiness (USD (P&R))

DoD Directive 5149.2, Senior Readiness Oversight Council (July 2002, certified current November 2003)

DoD Directive 7730.65, Department of Defense Readiness Reporting System (June 2002, certified current April 2007)

OPNAV Instruction 3501.36, Defense Readiness Reporting System - Navy (DRRS-N) (January 2008)

E.O. 9397 (SSN) as amended

Department of Navy, OPNAVINST 3501.383, 20 October, 2010. Fleet Readiness Reporting Guidance

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.

RCRP is a readiness reporting system based on Mission Essential Tasks (METs) which provides a standardized, enterprise-wide capability for the Navy Expeditionary Combat Command (NECC) operating forces to measure, display and report the readiness status of personnel, equipment, supply, training and ordnance resources and meet Defense Readiness Reporting System-Navy (DRRS-N) requirements. RCRP provides Commanders at appropriate levels within NECC with the ability to visualize the readiness of their units and subordinate units based on Chain of Command construct and associated permissions/roles in response to mission needs.

RCRP provides a full range of capabilities to satisfy the readiness and logistics business needs of NECC operating forces. The RCRP initiative creates a near real time, capability based readiness reporting system for NECC based on Mission Essential Tasks (METs). RCRP provides NECC Forces a standardized, enterprise-wide capability to: measure, display and report the readiness status of NECC Force PESTO (Personnel, Equipment, Supply, Training, Ordnance) resources to DRRS-N (Defense Readiness Reporting System-Navy); Support adaptive force packaging by granulating NECC's capabilities and supporting resources to the level required to provide the necessary visibility and supporting readiness picture; Stimulate cost-wise behavior and shape future investment by providing a capability for future resource planning based on resource priority in the context of capabilities; Provide metrics-based planning support Improve the balance of readiness and cost by tying readiness to cost. RCRP enables the central management and/or aggregation of PESTO resources while providing Commanders at all levels within NECC the ability to visualize the readiness of its unit at several levels to respond to mission needs. RCRP is currently in phase II of spiral development. RCRP is deployed on both NIPRNet and SIPRNet, and is utilizing Navy authoritative data sources for PESTO information. The initial releases of RCRP are limited to manual data import/load techniques derived from Navy Training Information Management System (NTIMS), NFEELC TOA, TFMMS, and DRRS-N as authoritative data sources. Plans for future releases are to automate data transactions with these authoritative data sources as well as to incorporate additional Navy PESTO authoritative data resources such as TFMMS, PFOM, MFOM, OFOM, NSIPS, NTMPS, OIS, NAVICP, EDE (NTMPS / CeTARS, NIRM, TWMS, RHS, DCPDS, MMRS, PRIMS), SNAP / Microsnap / R-SUPPLY, PRMS Database and GFM. The RCRP system is hosted at DISA DECC Mechanicsburg.

PII collected and maintained in RCRP includes: Name, truncated SSN, medical information, disability information, education information.

Personnel information: Enlisted/Officer (profile type), Permanent Duty Station, Current Assignment (short name), Unit Identification Code (UIC), Rating, Grade, Active Duty Start Date (ADSD), Projected Rotation Date (PRD), End Active Obligated Service (EAOS), Estimated Date of Loss (EDL), Navy Enlisted Code (NEC), Distributed Navy Enlisted Code (DNEC), Navy Officer Billet Classification (NOBC), Designator, Unavailable for Tasking, Sub Specialty, Rank, Additional Qualification Designation, Billet Information, Pay Entry Base date.

Personal Gear Issued: Description, National Stock Number (NSN), Allowance, Size.

Education and Professional Transcript: Course Identification Number (CIN/CSE ID), Course Name, Graduation Date, Expiration, Positions, Skills and Qualification Certification License (QCL).

Medical, Disability and Individual Readiness: Available for Tasking, Deployability (ITEMPO), Individual Augmentee (IA), Temporary Additional Duty (TAD), Accounting Category Code (ACC), Physical Readiness Test (PRT).

Additionally the system maintains RCRP user account and authorization information (user identifier, user role/privileges and security questions).

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

The risks associated with RCRP are inherent to computer systems in general, and primarily result from a compromise to data confidentiality, integrity, or availability from threats. Threats include unauthorized access by hackers, disgruntled employees, or state sponsored information warfare. Within RCRP these risks are addressed through the application of information assurance controls mandated by Department of Defense (DoD) Directive 8500.1 and DoD Instruction 8500.2. The application of these controls to the RCRP system has been evaluated and the system is certified and accredited to operate within the specified environment. IA Controls addressing administrative, physical, and technical protections are applied to RCRP, including physical security and environmental controls, authentication and access, encryption, training, and administrative policy and procedures. Contingency plans, including incident response plans, are tested at least annually.

Computerized records are maintained in a controlled area accessible only to authorized personnel. Entry to these areas is restricted to those personnel with a valid requirement and authorization to enter. Physical entry is restricted by the use of locks, guards, and administrative procedures. Access to personal information is restricted to those who require the records in the performance of their official duties. Access to personal information is further restricted by the use of passwords and Common Access Card (CAC). All individuals to be granted access to this system of records are to have received Information Assurance and Privacy Act 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.

without that information.

(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?

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 data contained in the system for mission related use is provided from interfaces with other systems or directly from the individual. The information is required to determine unit readiness, individual readiness, and to fulfill operational mission requirements.

For personnel requesting user account access, PII data is required for administrative purposes to determine need-to-know and establish authorized privileges. Since PII data is required for account access, individuals who elect not to provide the data will be denied user access.

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

Upon login to the system and when a user initiates an account request a Privacy Act Statement is displayed to the user.

format.

Reports and screens containing PII data are labeled with a banner stating the Privacy sensitive nature of the information.

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.