



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Readiness and Cost Reporting Program (RCRP)

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
- 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.

- 10 U.S.C. 5013, Secretary of the Navy
- 10 U.S.C. 117, Readiness reporting system: establishment; reporting to congressional committees (January 2004)
- DOD Directive 5149.2, Senior Readiness Oversight Council (July 2002)
- DOD Directive 7730.65, Department of Defense Readiness Reporting System (June 2002)
- OPNAV Instruction 3501.36, Defense Readiness Reporting System - Navy (DRRS-N) (January 2008)
- E.O. 9397 (SSN), as amended

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 provides capabilities to satisfy the readiness and logistics needs of Navy Expeditionary Combat Command (NECC) operating forces. RCRP is a readiness reporting system based on Mission Essential Tasks (METs) which provides NECC Forces with a standardized, enterprise-wide capability 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. The type of information collected consists of personal and assignment information (name, partial Social Security Number (last 4 of SSN), duty station, Unit Identification Code, rate, grade, designator, Navy Enlisted Code, Navy Officer Billet Classification Code, Active Duty Start Date, Projected Rotation Date, End Active Obligated Service, gear issued), qualifications (courses, graduation dates and expirations) and readiness related status information (medical readiness, physical readiness, administrative status, availability, deployability). 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 such as unauthorized access by computer hackers, disgruntled employees, or state sponsored information warfare, or as a result of acts of nature such as fire, flood, etc. 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. Information Assurance Controls are applied to the RCRP system to address a broad range of administrative, physical and technical data protections including: physical security and environmental controls, authentication and access, confidentiality (encryption), training, and administrative policies and procedures.

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 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 in order to determine unit and individual readiness 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.

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in SECNAVINST 5211.5, Code of Federal Regulations (CFR) Title 32 National Defense part 701; or may be obtained from the system manager.

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 in order to determine unit and individual readiness 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.

The Navy's rules for accessing records, and for contesting contents and appealing initial agency determinations are published in SECNAVINST 5211.5, 32 CFR part 701; or may be obtained from the system manager.

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.

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

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

Initial Collection of PII information is obtained through system integration with various data sources. No manual entry being performed.

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.