# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| |
|---|
| Fleet and Family Readiness System (FFRS) |
| Department of the Navy - CNIC |

## 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: 14923 DITPR DON ID: 22455
- ☐ **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** UII: 007-000004004

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** N01750-1

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** OMB package confirmed to be with OPNAV DNS-15.

**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:

10 U.S.C. 5013, Secretary of the Navy
OPNAVINST 1750.1G, Navy Family Ombudsman Program

**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 Fleet and Family Readiness Systems (FFRS) is the system currently used within Commander, Navy Installations Command (CNIC) N9, and consists of all of the required applications that support core business functions for Fleet and Family Readiness (FFR) Programs, including those used for centralized program administration, management of digital video, tracking, monitoring, data gathering and reporting. The applications that make up the FFRS include the Ombudsman Registry, Navy Motion Picture Service Movie Module, CNIC Video Manager, Navy Fitness, Duty In Japan and N9 E-mail Marketer. FFRS is a Web-based secured system operating within the CNIC Service Delivery Point (SDP) Norfolk.

The Ombudsman Registry is the only application within the FFRS that will collect PII from individuals. It centralizes program administration of the Ombudsman network; 3,925 commands that would consist of about 5,364 registrants (commanders, Ombudsmen and Coordinators) who are geographically dispersed throughout the world. The application provides Ombudsmen with program information; communication during natural disasters and crisis, collects program statistics and workload data; and maintains records of program training received. Statistics provided from collection shows command officers the issues and concerns of command families, trends during deployment versus non-deployment periods, and training which may be beneficial to the command and families. In addition, it allows CNIC to deliver real-time communication and information to commanders, Ombudsmen and Ombudsman coordinators.

The application contains the following PII: name, gender, personal cell phone number, home telephone number, mailing/home address and personal e-mail address and rank of commanding officers and/or their appointed representatives, command name and address.

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

PII is collected and stored in the FFRS secured host Web-based system. PII data is displayed on workstation monitors, which could be inadvertently viewed by other DoD employees. All CNIC employees must complete PII and Information Assurance training. To avoid compromise, workstations "time out" and monitors darken if periods of inactivity are exceeded. This keeps unattended workstations from being left on for long periods with data exposed. The potential privacy risks are from authorized system users with malicious intent, users with legitimate electronic access to data and outsiders who gain illegitimate access to the system or network where the server resides. These risks are mitigated by restricting a user's rights in FFRS to those functions required to perform their job, buy using SSL encryption and by following DoD Information Assurance policies.

**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. CNIC N9

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. United States Coast Guard

☐ **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.

The Ombudsman position is voluntary; however, in accordance with OPNAVINST 1750.1G 5d(2)b, commanders are required to register their command Ombudsmen in the registry. Failure to provide the required information would prohibit acceptance of the individual into the Ombudsman program.

(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.

According to OPNAVINST 1750.1G 5d(3)

Commanding officers and commanders shall: Accept volunteer services from the Ombudsman per reference (i) by completing DD 2793 (Rev. 5-09), Volunteer Agreement for Appropriated Fund Activities and Non-appropriated Fund Instrumentalities with the Ombudsman.

**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.

A Privacy Act statement is provided and staff informs the individual of the data that is being requested and explains what the Privacy Act statement addresses. The staff addresses the legal authority for requesting PII information from the individual and the principle purpose to the collection of PII from which their information will by used. They are also informed of the routine uses that may be made of their information, other disclosure of their information, that disclosure of PII is voluntary and they are asked to sign the Privacy Act statement.

**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.**