



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Fleet and Family Support Management Information System (FFSMIS)
Department of the Navy, Commander, Navy Installations Command (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
- 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.

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; E.O. 9397 (SSN); DoD Directive 6400.1, Family Advocacy Program; 6400.1-M, Manual for Child Maltreatment and Domestic Abuse Incident Reporting System; Secretary of the Navy Instruction 1752.3B, Family Advocacy Program; OPNAVINST 1752.2B, Family Advocacy Program; OPNAVINST 1700.9E, Child and Youth Programs; and DoDI 1402.5, Criminal History Background Checks on Individuals in Child Care Services.

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 electronic data collected in FFSMIS system provides pertinent case-related information to DoD and DON officials, for specific case intervention in abuse and /or neglect incidents. FFSMIS is a case management system and it is use to provide Defense Manpower Data Center (DMDC) with data from Navy's Central Registry.
DD Form 2486, form used for reporting in FFSMIS (application contains the following name, pay grade/rank, Social Security Number (SSN), service type, resource type, gender, date of birth, marital status, branch of service, alleged victim information, sponsor information, alleged offender information and health treatments provided etc).

(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 FFSMIS, secured host web based system . PII data is displayed on workstation monitors and produced in hard copy reports which could be inadvertently view by other DoD employees and FFSC customers. All Fleet and Family Support personnel must take 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 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 FFSMIS to those functions required to perform their job, by using SSL encryption, and by following DOD Information Assurance policies. If the information is provided verbally, there is a risk that it will be overheard by others waiting to be serviced. This risk is mitigated by reading the information directly from the CAC.

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.

Data Manpower Defense Center (DMDC)
Office of Secretary of Defense (OSD)
Military Services: Army, Air Force, Marine Corps

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.

Clients have the opportunity to provide or decline the provision of personal information at the introduction of treatment. The individual provides consent to collection of personal information by signing privacy act and consent forms prior to treatment. The client has the right also to refuse services to the extent permitted by law and Government regulations and to be informed of the consequences of his or her refusal. Individuals may also object to collection of their PII by the following procedures outline in the system of record notice N01752-1.

(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.

Specific uses of PII information is explained to individuals by FAP Clinicians and FFSP spouses during the verbal and /or written application process. A Privacy Act statement is provided to individual for the use of their PII. Individuals may also object to specific use of their PII by following the procedures outlined in the system on records notice N01752-1. Disclosure is voluntary failure to provide pertinent information may hinder or prevent the Fleet and Family Service Centers (FFSC) from being able to assist them.

(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.

When the individual enters the FFSC for their intake brief, the Privacy Act Statement is provided to the client. The Fleet and Family Support Center (FFSC) staff informs the individual of the data that is being requested and explains what the Privacy Act statement addresses. The staff addresses the legal authorities for requesting PII information from them, the principal purpose of the collection of PII for which their information will be used. They are also informed of the routine uses which may be made of their information, other disclosure of their information, and that disclosure of PII is voluntary. Once the FFSC staff member has explained the contents of the Privacy Act Statement and routine uses of the information they will be 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.