PRIVACY IMPACT ASSESSMENT (PIA)

For the

Fleet and Family Support Management Information System (FFSMIS)
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: 189 DITPR DON ID: 20760
☐	**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 007-000001980

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 N01752-1

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

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:

5 U.S.C. 301, Departmental Regulations
DoD Directive 6400.1, Family Advocacy Program
DoD 6400.1-M, Manual for Child Maltreatment and Domestic Abuse Incident Reporting System
DoD Directive 6400.2
Secretary of the Navy Instruction 1752.3B, Family Advocacy Program
OPNAVINST 1752.2B, Family Advocacy Program
BUMEDINST 6320.22
MCO 1752.3B (FAP SOP)
E.O. 9397 (SSN), as amended.

Other authorities:

OPNAVINST 1700.9E, Child and Youth Programs
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 Fleet and Family Support Management Information System (FFSMIS) is an independent server-based management information system. FFSMIS provides a web-based NMCI compliant, relational database with a full range of data gathering, collation and reporting capabilities for use in measuring program service delivery outputs and demographic metrics necessary for the Program Objectives Memorandum (POM) resource allocation process, record systems maintenance for documentation of sensitive, privacy act governed individualized service delivery and to comply with legislative and regulatory reporting requirements. The program maintains referential integrity for use by CNIC HQ, Fleet & Family Support Centers (FFSCs) and Family Advocacy Program (FAP) Centers at 71 worldwide service delivery sites for data input and management of the Fleet and Family Support Programs (FFSP).

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.

Personal information in FFSMIS includes: Name, SSN, DoD ID Number, Gender, Race/Ethnicity, Birth Date, Personal Cell Telephone Number, Home Telephone Number, Mailing/Home Address, Spouse Information: name, date of birth, age, and current address; Marital Status, Child Information: name, date of birth, age, current address, and number of children; Financial Information: financial welfare; Disability Information: type of disability; Law Enforcement Information: incident reports, police reports, and case notes; Employment Information: work history.

(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. CNIC HQ, Fleet & Family Support Centers (FFSCs) and Family Advocacy Program (FAP) Centers at 71 worldwide service delivery sites

☐ **Other DoD Components.**

Specify. Data Manpower Defense Center (DMDC)

Office of Secretary of Defense (OSD)
Military Services: Army, Air Force

☐ **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.

(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. 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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

☒ Name	☐ Other Names Used	☒ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☒ Other ID Number
☐ Citizenship	☐ Legal Status	☒ Gender
☒ Race/Ethnicity	☒ Birth Date	☐ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☐ Personal Email Address
☒ Mailing/Home Address	☐ Religious Preference	☐ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☒ Spouse Information
☒ Marital Status	☐ Biometrics	☒ Child Information
☒ Financial Information	☐ Medical Information	☒ Disability Information
☒ Law Enforcement Information	☒ Employment Information	☐ Military Records
☐ Emergency Contact	☐ Education Information	☐ Other

If "Other," specify or explain any PII grouping selected.

Spouse Information: Married or Single
Child Information: Gender (Male or Female)
Financial Information: Personal Financial Counseling
Law Enforcement Information: Local Police Checks
Employment Information: Employed or unemployed
Other: pay grade/rank, service type, resource type, branch of service, alleged victim information, sponsor information, alleged offender information and health treatments provided.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

The PII data collected from our clients with professional staff input.

(3) How will the information be collected? Indicate all that apply.

☒	Paper Form	☒	Face-to-Face Contact
☒	Telephone Interview	☒	Fax
☒	Email	☒	Web Site
☐	Information Sharing - System to System		
☐	Other		

If "Other," describe here.

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Verification and identification. FFSMIS PII data is used to verify status in the Department of the Navy for incidents, case closures, reports for domestic abuse for the Department of the Navy.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Both mission-related and administrative. Intended use of PII collected is used for the Department of the Navy Family Advocacy Program case files regarding abuse or neglect of victims/offenders associated with DON and other Military Family Advocacy programs. PII data is used to validate data for incidents of domestic abuse; eligibility decisions, metrics, safely assessments for intervention plans for case review committees.

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. **Who has or will have access to PII in this DoD information system or electronic collection?** Indicate all that apply.

☒ Users ☒ Developers ☒ System Administrators ☒ Contractors

☐ Other

If "Other," specify here.

d. **How will the PII be secured?**

(1) Physical controls. Indicate all that apply.

☒ Security Guards	☒ Cipher Locks
☒ Identification Badges	☐ Combination Locks
☐ Key Cards	☐ Closed Circuit TV (CCTV)
☐ Safes	☐ Other

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

☒ User Identification	☐ Biometrics
☒ Password	☒ Firewall
☒ Intrusion Detection System (IDS)	☒ Virtual Private Network (VPN)
☒ Encryption	☒ DoD Public Key Infrastructure Certificates
☒ External Certificate Authority (CA) Certificate	☒ Common Access Card (CAC)

☐ Other

If "Other," specify here.

(3) Administrative Controls. Indicate all that apply.

☒ **Periodic Security Audits**

☒ **Regular Monitoring of Users' Security Practices**

☒ **Methods to Ensure Only Authorized Personnel Access to PII**

☒ **Encryption of Backups Containing Sensitive Data**

☒ **Backups Secured Off-site**

☐ **Other**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

☐ **Yes. Indicate the certification and accreditation status:**

☒	**Authorization to Operate (ATO)**	**Date Granted:**	20110616
☐	**Interim Authorization to Operate (IATO)**	**Date Granted:**	
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Collection, Use, Processing: Individual privacy risk is minimized to the greatest extent possible. The initial collection is completed by the FAP Clinicians during the application procedure. Pertinent information is limited to DoD and DON officials responsible for intervening in abuse and /or neglect incidents and is safeguarded. These files are highly sensitive and must be protected from unauthorized disclosure.

Retention and Disclosure: While records may be maintained in various kinds of filing equipment, specific emphasis is given to ensuring that the equipment areas are monitored or have controlled access. Access to records or information in the Central Registry is limited to those officials who have been properly screened and trained and/or have a need to know consistent with the purpose for which the information was collected. The threshold for `need to know' is strictly limited to those officials who are responsible for the identification, prevention, evaluation, intervention, treatment and rehabilitation of beneficiaries involved in abuse or neglect. Information maintained in computer databases requires password protection and/or Common Access Card (CAC) access. Computer terminals are located in supervised areas with access control.

All government employees and contractors accessing and maintaining PII data within the FFSMIS system are required to take PII training and sign disclosure statements.

Destruction: Data is destroyed in accordance with the Navy's Record Management Manual.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

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 FFSMIS, with its extensive collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.

FFSMIS operates on the Navy MWR CNIC Millington Network, there is a risk that security controls could be disabled for maintenance and other purposes. The risk would be that the security controls would not be reset.

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

FFSMIS is on a secure network protected by multiple firewalls, security scans and monitoring. The FFSMIS system is hosted on a secure Navy base in a secure building and hosting room. FFSMIS conforms requirements for software security updates, is electronically monitored and has tools to detect attacks and attempts at intrusion. FFSMIS contracts require contractors to utilize encryption for PII stored on workstations. FFSMIS contractors work in secure facilities and all contractors with access to FFAMIS have a National Agency Check with Written Inquiry (NACI) or secret clearance. Data for other than formal business use (training and system demonstrations) is scrambled eliminating PII content. All reports have disclosure statements.

The following controls are used to mitigate the risks:

a) Access Controls. Access controls limit access to the application and/or specific functional areas of the application. These controls consist of privileges, general access, password control and discretionary access control. Additionally, each user is associated with one or more database roles. Each role provides some combination of privileges to a subset of the application tables. Users are granted only those privileges that are necessary for their job requirements. The same roles that protect the database tables also determine which buttons and menu items are enabled for the user currently logged on.

b) Confidentiality. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

c) Integrity. This ensures that data has not been altered or destroyed in an unauthorized manner.

d) Audits. This includes review and examination or records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the application.

e) Training. Security training is provided on a continuous basis to keep users alert to the security requirements. Visual effects are used as constant reminders to ensure users always remain aware of their responsibilities.

f) Physical Security. This consists of placing servers that contain privileged information in a secure and protected location, and to limit access to this location to individuals who have a need to access the servers. An internal policy is set in place to ensure that there are always no less than two users present at a time when privileged information is being retrieved. Since the server and data reside within a DON establishment, the strict security measures set by the establishment are always followed.

FFMIS servers are located at SDP Norfolk VA.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature	BURKS.CATHERINE.J.1104994209 Digitally signed by BURKS.CATHERINE.J.1104994209 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=BURKS.CATHERINE.J.1104994209 Date: 2014.04.15 16:41:45 -05'00'
Name:	Catherine Burks
Title:	IA Specialist
Organization:	CNIC
Work Telephone Number:	901 874-4377
DSN:	882-4377
Email Address:	catherine.burks@navy.mil
Date of Review:	
Other Official Signature (to be used at Component discretion)	ANBIYA.ABDUL HAKIM.SHARIF.1031557840 Digitally signed by ANBIYA.ABDUL HAKIM.SHARIF.1031557840 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=ANBIYA.ABDUL HAKIM.SHARIF.1031557840 Date: 2014.04.16 10:40:26 -04'00'
Name:	Hakim S. Anbiya
Title:	Director, Command and Staff/Privacy Act Coordinator
Organization:	CNIC
Work Telephone Number:	202-433-2919
DSN:	288-2919
Email Address:	hakim.anbiya@navy.mil
Date of Review:	16 April 2014

Other Official Signature (to be used at Component discretion)	
Name:	
Title:	
Organization:	
Work Telephone Number:	
DSN:	
Email Address:	
Date of Review:	
Component Senior Information Assurance Officer Signature or Designee	FLOYD.CAROL.NANETTE.1054406696 Digitally signed by FLOYD.CAROL.NANETTE.1054406696 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=FLOYD.CAROL.NANETTE.1054406696 Date: 2014.04.16 07:59:36 -04'00'
Name:	Carol N Floyd
Title:	IAPM
Organization:	DON/CNIC
Work Telephone Number:	(202) 433-3602
DSN:	288-3602
Email Address:	carol.floyd@navy.mil
Date of Review:	4016-2014
Component Privacy Officer Signature	SHAW.MARY.P.1229597341 Digitally signed by SHAW.MARY.P.1229597341 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=SHAW.MARY.P.1229597341 Date: 2014.09.04 15:35:48 -04'00'
Name:	for Robin Patterson
Title:	Head, FOIA/Privacy Act Program Office (DNS-36)
Organization:	Office of the Chief of Naval Operations (CNO)
Work Telephone Number:	202-685-6545
DSN:	
Email Address:	robin.patterson@navy.mil
Date of Review:	

Component CIO Signature (Reviewing Official)	MUCK.STEVEN.ROBERT.1179488597 Digitally signed by MUCK.STEVEN.ROBERT.1179488597 DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USN, cn=MUCK.STEVEN.ROBERT.1179488597 Date: 2014.09.04 15:59:13 -04'00'
Name:	For Barbara Hoffman
Title:	Principal Deputy CIO
Organization:	Office of the Department of the Navy Chief Information Officer (DON CIO)
Work Telephone Number:	703-695-1842
DSN:	
Email Address:	barbara.hoffman@navy.mil
Date of Review:	3 September 2014

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.