PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Military Child Care (MCC)

2. DOD COMPONENT NAME:

Department of the Navy

3. PIA APPROVAL DATE:

Commander, Navy Installations Command (CNIC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [ ] From Federal employees and/or Federal contractors
- [x] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

MCC is an OSD-funded, Navy-sponsored, globally-accessible Child and Youth Program (CYP) web-based child care management system. All four military services, Air Force, Army, Marine Corps and Navy, use MCC. It is designed to address the child care needs of DoD service members, civilians and contractors worldwide. It is a singular website service that enables DoD customers to request Child and Youth services, programs to manage care, and leadership to obtain data related to child care demand. Additionally, the system manages registration, enrollment and subsidy payments for families using the Military Child Care in Your Neighborhood (MCCYN) fee assistance and Family Child Care programs. The system is used to manage FCC and Program Certification requirements, which includes conducting annual child and youth inspections, family program certification reviews and monthly family child care visits.
Elements of Pll potentially collected includes: Full name, date of birth, personal mobile and/or home telephone number, personal email address, home mailing address, emergency contact, employment information, branch of service and employer/command, pertinent medical & disability information (general questions with yes/no selections, yes opens free form comment box for self-disclosed input). SSN are not collected in this system.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

Information, to include elements of PII, is collected during applicant registration to validate DoD family status and to facilitate a detailed administrative search for child care services resulting in offering and placing qualified applicants with programs and providers that best suit the requesting family needs. Uploaded artifacts with potential to include elements of PII are used to support and validate child care site/ facility inspection results.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Consumers/Parents objecting to collecting elements of PII may choose not to participate in the on-line service. However, failure to register and provide required information results in the inability to process and/or provide military child care services.
Information collected, including PII elements, is required and integral to identify, vet, and certify child care service providers. Failure to provide required information disqualifies an applicant from participation in the program.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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.

Program applicants/participants effectively consent to the use of information provided in order to process requests for military child care

services when voluntarily providing required information during program registration through the on-line service (militarychildcare.com). For elements of PII not specifically or directly collected from individuals but derived from external sources or systems (e.g. derivative PII) and subsequently introduced (e.g. via uploaded attachment) - the original source/entity responsible for collecting the PII elements is likewise responsible for determining appropriateness and capability for individual consent to specific use(s) of the PII collected.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

1. AUTHORITY: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; DoD Instruction 6060.2, Child Development Programs; DoD Instruction 6060.4, Youth Programs; OPNAV Instruction 1700.9 series, Child and Youth Programs; Marine Corps Order 1710.30, Child and Youth Programs (CYP); and E.O. 9397 (SSN) as amended.

2. PRINCIPLE PURPOSES(S): To develop child care programs that meet the needs of children and families; provide child and family program eligibility and background information; and verify health status of children and verify immunizations.

3. ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To local, State and Federal officials involved in Child Care Services, if required, in the performance of their official duties relating to child abuse reporting and investigations. The DoD Blanket Routine Uses that appear at the beginning of the Navy's compilation of systems of records notices apply to this system.

4. DISCLOSURE: Voluntary. However, failure to provide requested information may impact eligibility for military child care facilities.

Introduction

This is a Department of Defense (DoD) interest computer system sponsored by the Office of Military Family Readiness Policy (OMFRP) Office of the Secretary of Defense Military Community and Family Policy as a public service. This statement details the steps we take to protect your personal information when you visit our website. It describes the personal information we collect, the purposes for which we use such information, and your choices regarding our use of it. By accessing our website, you are consenting to the information collection and use practices described in this privacy statement.

Our collection of information

Information collected directly from you. The personal information we collect may include the following. You are not required to provide any of this information, but if you do not, we may not be able to provide you the requested service.

contact details, such as your name, company/organization name, e-mail address, telephone, and physical address;
child care request information such as child name, date of birth, and date care is needed;
your e-mail communication preferences; and
information used to customize and facilitate your use of our websites, including login information.
Information collected automatically. We collect information about your visit to our sites, including what pages you view, the number of bytes transferred, the links you click, the materials you access, and other actions taken within the site. We also collect certain standard information that your browser sends to every website you visit, such as your Internet Protocol (IP) address, your browser type and capabilities and language, your operating system, the date and time you access the site, and the website from which you linked to our site.

Our use of information

We use your personal information to (1) manage the request for care process (e.g., waitlist) and (2) to inform you about the status of your child care request(s). Program staff may contact you directly or you may receive system-generated email notifications. You are able to opt-out of receiving many system generated emails.

Our use of cookies

Cookies are small files that websites save to your hard disk or to your browser's memory. We may use them to track the number of times you have visited the site, to track the number of visitors to the site, to determine and analyze visitors' use of our site, to store information that you provide such as your preferences, and to store technical information useful for your interactions with our website. We may use session cookies (cookies that are deleted when your browser session ends) to store your user ID, elements of your user profile, to facilitate your movement around our website and other information useful in administering the session. You have the ability to accept or decline cookies. Most Internet browsers automatically accept cookies, but you can usually modify your browser settings to decline cookies or to notify you when a cookie is being placed on your computer. If you choose to decline cookies, you may not be able to fully experience the features of our website or other websites that you visit.

MilitaryChildCare.com does not use the information associated with cookies to track individual user activity on the Internet outside Defense Department websites, nor does it share the data obtained through such technologies, without the user's explicit consent, with other departments or agencies.

Use of web analytics

This website uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and internet usage. Google may also transfer this information to third parties where required to do so by law, or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google. You may refuse the use of cookies by selecting the appropriate settings on your browser. By using this website, you consent to the processing of data about you by Google in the manner and for the purposes set out above.

Disclosure of your personal information

Except as described below, personal information you provide to MilitaryChildCare.com through our website will not be shared outside of MilitaryChildCare.com programs without your permission.

Disclosure in connection with child care requests. In connection with certain requests, we may disclose some or all of your personal information to promote effective communication and planning (e.g., Inclusion Action Team, Special Needs Review Team) and respond to your child’s individual needs.

Security

MilitaryChildCare.com is committed to protecting the security of your personal information. We use a variety of security technologies and procedures to help protect your personal information from unauthorized access, use, or disclosure. For example, we store the personal information you provide on computer systems with limited access that are located in facilities to which access is limited. For sites to which you login, it is your responsibility to ensure the security of your password and not to reveal this information to others.

Links to other sites

Our website may contain links to other sites such as school districts associated with your child care request. While we try to link only to sites that share our high standards and respect for privacy, we are not responsible for the content, security, or privacy practices employed by other sites.

Changes to this privacy statement

MilitaryChildCare.com may occasionally update this privacy statement. When we do, we will revise the "last updated" date at the top and bottom of the privacy statement.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

[x]	Within the DoD Component	Specify.	No system-to-system electronic data exchange pertains or occurs. Authorized US Navy and Marine Corps Child and Youth Programs (CYP) employees supporting CYP program mission objectives (e.g. program administrators; inspectors etc.); have controlled access to stored data on a need-to-know basis.
[x]	Other DoD Components	Specify.	Office of SECDEF (OSD); US Army CYP; US Air Force CYP; DLA.
[ ]	Other Federal Agencies	Specify.	
[ ]	State and Local Agencies	Specify.	

☒	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	American Systems Corp. (ASC) Property/program information management accountability requirements include: Compliance with all DoD Pll and security requirements. The program must adhere to Department of defense (DoD) mandates and best practices for securing and safeguarding Personally Identifiable Information (PII). Pll policies are outlined in OMB-M-06-16; OMB-M-06-19; and DoD instruction 8500.2. These Mandates and best practices are included in the SECNAV Instruction 5211.5E or CN IC Instruction 5211.1 or review in the Department of the Navy Personally Identifiable Information (PII) training module. The Online system is to include servers that must comply with DoDI8500.2. With these responsibilities contractors should ensure that their employees: Safeguard DON information to which their employees have access at all times. Obtain DON management's written approval prior to taking any DON sensitive information away from the office. The DON manager's approval must identify the business necessity for removing such information from the DON facility. Contractors undergo National Agency Checks and all personnel who use or view the data are required to complete the DoD privacy training annually and complete the CompTIA Sec + Certification successfully. Access to data is granted by system permissions. The FAR Privacy clauses are included in the contract. ICF, International is the software developer and software support contractor. However, multiple support contracts and contractor support personnel may be assigned depending on the separate contracts established by the respective service components (e.g., Air Force, Marine Corps).Authorized care givers are contracted separately. Standard contract requirements include language for contractors to undergo an appropriate background investigation; complete annual privacy act training, and complete annual security training to include proper information handling, and acceptable use of government Information Technology (IT). data are required to complete the DoD privacy training annually. Access to data is granted by system permissions.
☒	Other *(e.g., commercial providers, colleges).*	Specify.	Authorized care givers (end users of the system) are contracted separately. Standard contract requirements include language for contractors to undergo an appropriate background investigation. End user access is restricted by system permissions.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- ☒ Individuals
- ☐ Databases
- ☐ Existing DoD Information Systems
- ☐ Commercial Systems
- ☐ Other Federal Information Systems

No specific information systems, databases, or collection of records (e.g. paper-based file system) - but elements of PII can potentially be derived from an alternate source and subsequently introduced via uploaded attachment, for example.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- ☐ E-mail
- ☐ Official Form (*Enter Form Number(s) in the box below)*
- ☐ Face-to-Face Contact
- ☐ Paper
- ☐ Fax
- ☐ Telephone Interview
- ☐ Information Sharing - System to System
- ☒ Website/E-Form

☒ Other *(If Other, enter the information in the box below)*

In the course of an inspection, inspectors can potentially collect a supporting artifact that contains one or more elements of PII and subsequently introduce/upload the artifact (e.g. via an attachment) to the MCC web-based IT system - where it is stored in an DoD-compliant encrypted database.

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier NM01754-3

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-NU-2015-0001-0031

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Old SSICs 1754.1b and 1700 updated SSIC 1000-34. TEMPORARY: Cutoff at CY. Destroy when 3 years old.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORN NM01754-3, DON Child and Youth Program (May 27, 2010, 75 FR 29728), authorities:
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
DoD Instruction 6060.2, Child Development Programs
DoD Instruction 6060.4, Youth Programs
OPNAV Instruction 1700.9 series, Child and Youth Programs
Marine Corps Order P1710.30E, Children, Youth, and Teen Program (CYTP)
E.O. 9397 (SSN), as amended.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☐ No ☒ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Military Child Care (MCC) is part of Child and Youth (CYP) Programs. The data collection is included in the CYP OMB Control Number packet being reviewed by the CNIC Privacy Compliance Officer for submission.

SECTION 2: PII RISK REVIEW

a. What PII will be collected *(a data element alone or in combination that can uniquely identify an individual)**?** (Check all that apply)*

☐ Biometrics	☒ Birth Date	☒ Child Information
☐ Citizenship	☒ Disability Information	☐ DoD ID Number
☐ Driver's License	☒ Education Information	☒ Emergency Contact
☒ Employment Information	☒ Financial Information	☒ Gender/Gender Identification
☒ Home/Cell Phone	☒ Law Enforcement Information	☐ Legal Status
☒ Mailing/Home Address	☒ Marital Status	☒ Medical Information
☐ Military Records	☐ Mother's Middle/Maiden Name	☒ Name(s)
☒ Official Duty Address	☒ Official Duty Telephone Phone	☐ Other ID Number
☐ Passport Information	☒ Personal E-mail Address	☐ Photo
☐ Place of Birth	☐ Position/Title	☐ Protected Health Information (PHI)[1]
☐ Race/Ethnicity	☐ Rank/Grade	☐ Religious Preference
☐ Records	☐ Security Information	☐ Social Security Number (SSN) *(Full or in any form)*
☒ Work E-mail Address	☒ If Other, enter the information in the box below	

Spouse Information: Name (First, Last), Address; Phone Number, Email, Employer; Employment Status; Emergency Contact.
Child information: Name, Parent(s), Address, Grade, School information (school they attend), DOB/Projected DOB, special needs.
Medical Information: Flu shot received (Provider)
Disability Information: Level of Special Need (Child)
Law Enforcement Information: Have you ever been arrested or charged for a crime involving a child victim, a sex crime, a substance abuse felony, or a violent crime? Yes/No. Have you ever been asked to resign a position or been decertified from a position for a sexual offense? Yes/No
Education Information: Highest Level of Education Received, Degree (if attended college)
Support and Accommodations (includes medical information): general question with yes/no selection, yes opens free form comment box for input
Employment information: Branch of Service (mandatory), Employer/ Command (mandatory)-free form field, employment type (active duty, civilian or reserve (mandatory), Employment Status, Have you ever been asked to resign a position or been decertified from a position for a sexual offense? Yes/No
For Providers only Flu shot date and if Health Screening was done Y/N information is collected.
For Financial information only household income summary is collected which is used to determine service rates.
Disability information is required in order to accommodate special needs.

If the SSN is collected, complete the following questions.

(*DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

☐ Yes ☒ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

☐ Yes ☐ No

b. What is the PII confidentiality impact level[2]? ☒ Low ☐ Moderate ☐ High

[1]The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2]Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

- ☒ Cipher Locks
- ☐ Combination Locks
- ☒ Key Cards
- ☒ Security Guards
- ☒ Closed Circuit TV (CCTV)
- ☒ Identification Badges
- ☐ Safes
- ☐ If Other, enter the information in the box below

MCC is a web-based application consisting entirely of virtual servers hosted at the DISA DECC Mechanicsburg, PA facility, on an approved DoD Information Network (DoDIN) enclave from which applicable site-specific physical and environmental security controls are inherited. Evidence supporting security control inheritance and the compliance status of all applicable site-specific physical and environmental security controls is available for review in the eMASS (10768) record.

(2) Administrative Controls. *(Check all that apply)*

- ☒ Backups Secured Off-site
- ☒ Encryption of Backups
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☒ Periodic Security Audits
- ☒ Regular Monitoring of Users' Security Practices
- ☐ If Other, enter the information in the box below

MCC is a web-based application consisting entirely of virtual servers hosted at the DISA DECC Mechanicsburg, PA facility, on an approved DoD Information Network (DoDIN) enclave from which a portion of applicable administrative security controls are inherited. Evidence supporting security control inheritance and the compliance status of all applicable and implemented administrative security controls is available for review in the eMASS (10768) record.

(3) Technical Controls. *(Check all that apply)*

- ☐ Biometrics
- ☒ Encryption of Data at Rest
- ☒ Firewall
- ☒ Role-Based Access Controls
- ☒ Virtual Private Network (VPN)
- ☒ Common Access Card (CAC)
- ☒ Encryption of Data in Transit
- ☒ Intrusion Detection System (IDS)
- ☒ Used Only for Privileged (Elevated Roles)
- ☐ If Other, enter the information in the box below
- ☒ DoD Public Key Infrastructure Certificates
- ☒ External Certificate Authority Certificates
- ☒ Least Privilege Access
- ☒ User Identification and Password

NIST/FIPS-compliant encryption of Data in Transit and Data at Rest. MCC is a web-based application consisting entirely of virtual servers hosted at the DISA DECC Mechanicsburg, PA facility, on an approved DoD Information Network (DoDIN) enclave from which a portion of applicable technical security controls are inherited. Evidence supporting security control inheritance and the compliance status of all applicable and implemented technical security controls is available for review in the eMASS (10768) record.

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

The NIST SP 800-53 Rev 4 - security control Privacy Overlay has been applied.

SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool[3]?

[X]	Yes, DITPR	DITPR System Identification Number	DITPR-DON ID: 22914
[ ]	Yes, SIPRNET	SIPRNET Identification Number	
[X]	Yes, RMF tool	RMF tool Identification Number	eMASS: 10768
[ ]	No		

If “No,” explain.

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, “Risk Management Framework for DoD Information Technology”.

Indicate the assessment and authorization status:

[X]	Authorization to Operate (ATO)	Date Granted:	3/19/2019
[ ]	ATO with Conditions	Date Granted:	
[ ]	Denial of Authorization to Operate (DATO)	Date Granted:	
[ ]	Interim Authorization to Test (IATT)	Date Granted:	

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

[ ] Yes [X] No

If "Yes," Enter UII _____ If unsure, consult the component IT Budget Point of Contact to obtain the UII

[3]Guidance on Risk Management Framework (RMF) tools (i.e., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

a. Program Manager or Designee Name	Diane Brewer	(1) Title	Progam Manager
(2) Organization	CNIC (N926)	(3) Work Telephone	901-830-4049
(4) DSN		(5) E-mail address	Diane.Brewer@navy.mil
(6) Date of Review		(7) Signature	BREWER.DIANE.LYNN.1067582957 Digitally signed by BREWER.DIANE.LYNN.1067582957 Date: 2021.09.09 09:03:42 -04'00'
b. Other Official *(to be used at Component discretion)*		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
c. Other Official *(to be used at Component discretion)*	Hakim S. Anbiya	(1) Title	Privacy Compliance Officer
(2) Organization	CNIC	(3) Work Telephone	202-433-4325
(4) DSN	288-4325	(5) E-mail address	abdul-hakim.s.anbiya.civ@us.navy.mil
(6) Date of Review	09/20/21	(7) Signature	ANBIYA.ABDUL-HAKIM.S.1031557840 Digitally signed by ANBIYA.ABDUL-HAKIM.S.1031557840 Date: 2021.09.20 11:29:57 -04'00'
d. Component Privacy Officer (CPO)		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

e. Component Records Officer	Karolina Lewandowska	(1) Title	Command Records Manager
(2) Organization	CNIC HQ	(3) Work Telephone	202-433-6515
(4) DSN	288-0895	(5) E-mail address	karolina.l.lewandowska.civ@us.navy.mil
(6) Date of Review	09/09/21	(7) Signature	LEWANDOWSKA.KAROLINA.L.1515237808 Digitally signed by LEWANDOWSKA.KAROLINA.L.1515237808 Date: 2021.09.09 10:44:07 -04'00'
f. Component Senior Information Security Officer or Designee Name	Carol Floyd	(1) Title	CYPM
(2) Organization	DON/CNIC	(3) Work Telephone	(202) 433-3602
(4) DSN	284-3602	(5) E-mail address	carol.floyd@navy.mil
(6) Date of Review:	09/09/21	(7) Signature	FLOYD.CAROL.NANETTE.1054406696 Digitally signed by FLOYD.CAROL.NANETTE.1054406696 Date: 2021.09.09 10:13:06 -04'00'
g. Senior Component Official for Privacy (SCOP) or Designee Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	
h. Component CIO Reviewing Official Name		(1) Title	
(2) Organization		(3) Work Telephone	
(4) DSN		(5) E-mail address	
(6) Date of Review		(7) Signature	

Publishing: Only Section 1 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: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

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 Section 1.