PRIVACY IMPACT ASSESSMENT (PIA)

For the

Career Management System - Interactive Detailing (CMS-ID)
Department of the Navy - SPAWAR - PMW 240

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: 8572 DITPR DON ID: 21701
☐	**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: 007-000003872

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 N01306-1

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
10 U.S.C. 5013, Secretary of the Navy
E.O. 9397 (SSN), as amended.

For Reserve Personnel, the manual that specifically authorizes the collection of information by this system is the Navy Reserve Personnel Manual (RESPERSMAN) (dtd 5 Jun2012) previously called COMNAVRESFORINST 1001.5f. The RESPERS M-1001.5 is issued under Navy Regulations. 1990 Article 0105, for direction and guidance, and contains administrative procedures for Drilling Reservists and participating members of the Individual Ready Reserve within our Navy in Sections 1000-010, 1300-010, and 1306-010 . Also outlined in Career Management System-Interactive Detailing (CMS-ID) Active/Reserve Integration (ARI) Functional Requirements Document dtd 08Feb2007.

For Active Duty Personnel, the manual that specifically authorizes the collection of information by this system is the Military Personnel Manual issued by Navy Personnel Command (NPC)(http://www.public.navy.mil/bupers-npc/reference/milpersman/1000/1300Assignment/Pages/default.aspx) in Sections 1306-100, 1306-104, 1306-110, and 1306-116. NPC's Distribution Guidance Memorandum (DGM) #2013-01 (https://mpte.portal.navy.mil/sites/NPC/restricted_documents/Shared%20Documents/DGM/DGM%202013-01.PDF020) call out the use of CMS-ID. Also outlined in Career Management System-

Interactive Detailing (CMS-ID) Spiral 0 Functional Requirements Document dtd 22Mar2006.

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.

Purpose -To assist Navy officials (government and designated contractors) in the initiation, development, and implementation of policies pertaining to enlisted personnel assignment, placement, retention, career enhancement and motivation, and other career related matters to meet manpower allocations and requirements. This system primarily displays a listing of available billets from which a Sailor or designated representative can submit a request for transfer and be assigned in the billet.

PII collected: Name, SSN, DOB are used to verify the Sailor's identity and access privileges and to locate the Sailor's records within the system. Contact information (Personal Cell Telephone Number, Home Telephone Number, Personal email address, and Mailing/Home Address) is used to contact the Sailor outside of the system (in event the Sailor does not have immediate access). Citizenship,Gender, Marital Status, Military Records, Citizenship, DoD ID, Security Clearance, and Education Information: education level and degree completion; are all used to assess the Sailor's fit for a potential job.

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

Potential threats/risk that may impact the integrity, availability and confidentiality of the CMS-ID system include hardware/software failure, and fire wall issues. These risks are mitigated through the use of DoD PKI certificates for server and client authentication. Logins to the system are controlled by the application. User authentication and role-based authorization are implemented to grant access to CMS-ID. All external communications to the web server are protected by an external firewall, host address block / allow lists and HTTP over SSL encryption. An outer firewall interface will require HTTP over SSL opened inbound to the web servers. System logins are limited, in general, to administrators, developers, and authorized users. The production database server resides within the Production Private Access Zone of the EDMZ.
- All systems are at risk because may be vulnerable to unauthorized intrusion and hacking. There are risk that CMS-ID with its collection of PII, could be compromised. Because of this possibility, appropriate security and access controls listed in this PIA are in place.
- Since CMS-ID operates on the NMCI 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". CMS-ID 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 CMS-ID. These individuals have gone through extensive background, employment investigations, and have a current System Authorization Access Request Navy (SAAR-N) on file.

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. Navy Personnel Command (NPC) and Commander Navy Reserve Force (CNRFC)

☐ **Other DoD Components.**

Specify. None

☐ **Other Federal Agencies.**

Specify. None

☐ **State and Local Agencies.**

Specify. None

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Methods Technology Solutions Contract N0003912C0107 and N0003912C0008

52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)
The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
52.224-2 PRIVACY ACT (APR 1984)
(a) The Contractor agrees to--
(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies--
(i) The systems of records; and
(ii) The design, development, or operation work that the contractor is to perform;
(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and
(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.
(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.
(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.
(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.
(3) "System of records on individuals," as used in this clause, means a group of any 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.
(End of clause)

☐ **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 is not collected directly from the individual.

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 is not collected directly from the individual.

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.	PII is not collected directly from the individual.

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.