PRIVACY IMPACT ASSESSMENT (PIA)

For the

Career Waypoint (C-Way)
Department of the Navy - BUPERS

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 12604/DITPR-DON ID 22085
☐	**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: 007-000003788

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 N01040-1 (Currently in routing at DNS)

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:

10 U.S.C 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN), as amended.

Additional authorities:

NAVADMIN 197/08 Rating Entry for General Apprentices (REGA)
NAVADMIN 267/05 General Detailed Transition Strategy
NAVADMIN 149/13 Career Navigator Program Announcement Part-1
NAVADMIN 150/13 Career Navigator Program Announcement Part-2
MILPERSMAN 1440-060 Perform to Serve (PTS) (To be superceded by MILPERSMAN 1160-140)
MILPERSMAN 1160-140 Career Waypoint (C-Way) Reenlistment (In Chop)
MILPERSMAN 1306-610 General Detail (GENDET) Targeted Enlistment Program (GTEP) (In Chop to become Professional Apprenticeship Career Track (PACT))
MILPERSMAN 1306-1500 Full Time Support (FTS)
MILPERSMAN 1306-1502 Eligibility Requirements and Application Procedures for Conversion and Recall to the Full Time Support (FTS) Program (In Chop to become Component Change Eligibility and Application Procedures Active Component (AC), Full Time Support (FTS), and Selected Reserve (SELRES))

MILPERSMAN 1306-1504 General Assignment Recall (To be cancelled and superceded by new MPM 1306-1502)
MILPERSMAN 1326-021 Navy Enlisted Reserve Component (RC) to Active Component (AC) Augmentation Program (To be cancelled and superceded by new MPM 1306-1502)
MILPERSMAN 1440-010 Change in Rating, Authorization (In chop to become Lateral Conversion)

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.

Career Waypoint (C-WAY) is the Navy's primary force shaping tool used to level rating manning from overmanned ratings to undermanned ratings for both rated and non-rated Sailors. It is also a rating quality and eligibility screening mechanism. C-WAY requires Sailor PII data to process C-WAY-Reenlistment (REEN) applications for retention, as well as qualify Sailors to rating conversions opportunities and Apprentices to rating designations, as part of mandatory Chief of Naval Personnel career counseling and retention programs, including C-WAY-REEN and C-WAY-Professional Apprenticeship Career Track (PACT).

PII collected by C-WAY is: Name, Social Security Number, Truncated SSN, DoD ID number, Citizenship: All immediate family members citizenship (to include parents), Armed Services Vocational Aptitude Battery (ASVAB) Scores and Gender are provided by Navy Standard Integrated Personnel System (NSIPS) and Corporate enterprise Training Activity Resource System (CeTARS). Race/Ethnicity, Birth Date, Place of Birth, Security Clearance, legal status, Education Information: Degree held, ASVAB scores, High school diploma, Navy Advanced Placement Test (NAPT) and Defense Language Aptitude Battery (DLAB) taken, Civil or military offenses, date of Non-judicial punishment (NJP), moral turpitude history, Medical Information: Color perception, drug/alcohol abuse, hearing acuity, speech impediments, vision (corrected and uncorrected), stereoscopic vision, physical fitness assessment (PFA) status, number of failed PFAs, Depth perception, Military Records: Pay Grade, and Geo-location of member. Vision and Hearing details about the Sailor's are provide by Command input (Service and Medical records review) and are stored in C-WAY for identifying Navy jobs for which the Sailor qualifies.

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

Privacy Act Information/PII contained within C-WAY could potentially be exposed to unauthorized users through malware infection, hacking, and/or phishing. These risks are mitigated by current system authority to operate (ATO), continuous monitoring and patching, mandatory user training, and implementation of DISA security technical implementation guides (STIG). Personally Identifiable Information(PII) is encrypted using Triple - Data Encryption Standard (Triple-DES) algorithm and stored in database tables. Additionally access to these database tables is restricted to authorized Data Center personnel with Security Clearance.

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. Authorized Users at all Navy Commands

☒ **Other DoD Components.**

Specify. Joint/Unified Commands and Defense Agencies

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. Hewlett Packard (HP) FAR52.224-1 Privacy Act Notification, FAR52.224-2 Privacy Act, and NAVSUP 5252.204-9400 Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information

☐ **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.

C-WAY does not collect PII data from individuals. C-WAY gets PII data from US Navy Data sources and local Command resources (Service and Medical record review) . This PII data is used in the C-WAY for user verification and to aid the Navy Career Counselors to provide counseling and guidance to Sailors about the C-WAY-REEN and C-WAY-PACT programs. C-WAY requires Sailor PII data to process C-WAY-REEN applications for retention as well as qualify Sailors to rating conversions opportunities and Apprentices to rating designations, as part of mandatory Chief of Naval Personnel career counseling and retention programs, including C-WAY-REEN and C-WAY-PACT. The JOIN survey (part of system accreditation boundary) collects the SSN as part of the survey. Required Privacy Act Statement is displayed prior to collection of SSN.

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.

C-WAY does not collect PII data from individuals. C-WAY gets PII data from US Navy Data sources and local Command resources (Service and Medical record review) . This PII data is used in the C-WAY for user verification and to aid the Navy Career Counselors to provide counseling and guidance to Sailors about the C-WAY-REEN and C-WAY-PACT programs. C-WAY requires Sailor PII data to process C-WAY-REEN applications for retention as well as qualify Sailors to rating conversions opportunities and Apprentices to rating designations, as part of mandatory Chief of Naval Personnel career counseling and retention programs, including C-WAY-REEN and C-WAY-PACT. The JOIN survey (part of system accreditation boundary) collects the SSN as part of the survey. Required Privacy Act Statement is displayed prior to collection of SSN.

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.

The JOIN survey (part of system accreditation boundary) collects the SSN as part of the survey. Required Privacy Act Statement is displayed prior to collection of SSN.

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.