PRIVACY IMPACT ASSESSMENT (PIA)

For the

My Education (My Education)
Department of the Navy - NETC

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: 14938 DITPR DON ID: 22452
☐	**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: 007-000004831

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 NMO1560-1; NM01500-2

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:

NM01560-1:

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

NM01500-2:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps function, composition
OPNAVINST 1510.10B, Corporate Enterprise Training Activity Resource System (CeTARS), Catalog of Navy Training Courses and Student Reporting Requirements
MCO 1580.7D Schools Inter-service Training
E.O. 9397 (SSN), as amended.

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.

My Education is an umbrella term for a suite of four applications: United Services Military Apprenticeship Program (USMAP), Navy College Management Information System (NCMIS), Joint Services Transcript (JST), and Non Resident Training Courses (NRTC).

USMAP is a web-based application that provides improved availability, timely and accurate reporting of apprentice data, and near real-time apprentice tracking to the Navy, Marine Corps, and Coast Guard community.
Active duty Navy, Marine, and Coast Guard personnel are eligible for USMAP and have access to the USMAP site for enrollment and processing of progress/status reports. USMAP transcripts are generated upon receipt and data is posted online for retrieval by members.
The system provides comprehensive data management of apprentice information from application to completion. Functions include:
-Management of resources and facilities
-Evaluating individual qualifications
-Determining training requirements and identifying individual training deficiencies
-Trade scheduling, trade enrollments, monitoring of individual records, recording member progress/status reports, analyzing and evaluating members records
-Ensuring the availability of applicable trades
-Assigning and controlling applicable trades
-Maintaining updated USMAP records and producing related USMAP documents
-Preparing statistical and other training reports
-Exchanging data with related automated systems
- Satisfying up-line reporting requirements as a by-product of performing local day-to-day USMAP functions.

NCMIS provides an on-line real-time system for authorizing tuition assistance (TA) for Navy, Marine and Coast Guard Service members and Sailors participating in the Graduate Education Voucher (GEV), Advanced Education Voucher (AEV) and Seaman to Admiral 21st Century (STA21) Programs. NCMIS captures both financial and program data for these programs accounting for more than $165 million in FY2014 tuition funds.
NCMIS provides on-line, real time financial and program management for the Navy College Program Afloat College Education (NCPACE) Program. NCMIS also captures program data for the Navy College Offices.
NCMIS is the Navy's sole source for degree information for the Navy Enlisted Master File and the Electronic Training Jacket as well as the source of academic course information for the Joint Services Transcript.
NCMIS has over 600 users at more than 150 locations.
NCMIS functions as the source of original entry for TA, GEV, STA21, AEV, and collects program and financial data for NCPACE, and Introductory Flight Syllabus. As a single integrated system, the NCMIS mission is to provide dynamic real time program operation voluntary education offices for Navy, Marine and Coast Guard, the Navy Virtual Education Center and Naval Reserve Officer Training Command units.

Joint Services Transcript (JST)
The JST is a web-based application that translates military training and occupations into recommended college credit as a military transcript. Unofficial transcripts are generated in real-time via the web site for Army, Navy, Marine Corps, Coast Guard and National Guard active and separated (veterans) personnel. Official military transcripts are released by individuals to post-secondary academic institutions.
Types of personal information collected by JST:
-Social Security Numbers (DoDID not available for separated personnel before DoDIDs existed)
-Training courses completed
-Job related positions held (Army Military Occupation Specialities, Navy Enlisted Rates and Classifications, Officer Designated and Billeting Codes, Coast Guard rates and officer codes, Marine Corps occupation specialities)
-Defense Language Proficiency Testing
-Certifications and Licenses

Non-Resident Training Course (NRTC)
NRTCs are self-study courses which may include exercises, lessons, or examinations designed to assist the student in acquiring the knowledge or skill described in the associated text. These self-study packages are designed to help students acquire Navy professional or military knowledge. The package normally consists of a course text and a set of course assignments, and may be delivered in printed or digital form and in some cases both. NRTCs provide active duty, reserve, and retired members of the U.S. Navy , Marines, U.S. Coast Guard, as well as DoN Civilians with valuable information.

Types of personal information collected by My Education suite of applications includes: Name, SSN (full and truncated), DoD ID number, Gender, Race/Ethnicity, Birth Date, Personal Cell Phone, Home Telephone Number, Personal Email, Mailing/Home Address, Financial Information, Military Records.

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

PII safeguards are described in the Certification and Accreditation (C&A) Plan. Data access is based on defined roles and access requires Common Access Card (CAC) or User Identification/Password identification/authentication to access records. Access is role-based and predicated on least privilege.

Physical access to the central computer operations area is provided on a need-to-know basis and to key card approved, CAC authorized, authenticated personnel only. Records are maintained in controlled access rooms or areas. Physical access to terminals is restricted to specifically authorized individuals who have a need-to-know. Password authorization, assignment, and monitoring are the responsibility of the functional managers.

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. Department of the Navy, Bureau of Naval Personnel, Navy Logistics Library, Naval Personnel Command, Navy Training Management Planning System, Marine Corps has access to their service data only

☒ **Other DoD Components.**

Specify. Army has access to their service data only; Department of Defense Advanced Automation System

☒ **Other Federal Agencies.**

Specify. Program Completion Letter provided to Dept of Labor with individuals name and completion date only; Dept of Transportation (Coast Guard) – members only have access to their own information

☒ **State and Local Agencies.**

Specify. Program Completion Letter provided to State Dept of Labor (North Carolina and Virginia) with individuals name and completion date only

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

Specify. N/A

☐ **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.

Personal information 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.

Personal information 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.

Personal information 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.