PRIVACY IMPACT ASSESSMENT (PIA)

For the

Department of Defense Voluntary Education System (DoDVES)
Department of the Navy - NETC - DANTES

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: 8700; DITPR DON ID: 21722
☐	**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: 007-000001255

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 NM01560-02 (December 11, 2006)

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	UII: 007-000001255
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:
110 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
Department of Defense Directive (DoDD) 1322.8
Voluntary Education Programs for Military Personnel and Department of Defense Instruction (DoDI) 1322.25
Voluntary Education Programs
E.O.9397 (SSN), as amended.

Other authorities:

PL 112-239 SEC 541 Troops To Teachers.

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.

Department of Defense Voluntary Education System (DODVES) supports the voluntary education functions of the DoD by administering nontraditional education programs, managing specified contracts for education services, providing educational and informational materials, conducting special projects and developmental activities, and performing other management and educational support tasks. Defense Activity for Non-Traditional Education Support (DANTES) fosters partnership between the civilian and military communities through agreements with testing agencies, colleges and universities, and educational associations. As a result, military students may use the same nationally recognized educational programs available to civilian students. DODVES Developed Applications. The Troops to Teachers (TTT) program is a DoD program established in 1994 to assist eligible military personnel transition to a new career as public school teachers in targeted schools in the US. The primary capabilities of the TTT application include participant registration, financial assistance, and referral and placement assistance. The TTT application determines eligibility potential participants based on pre-defined military service and education criteria. It manages registration data such as certifications, licensing, employment history, and teaching subject interest. TTT tracks financial assistance provided to participants. The purpose of the Jobs2Teach web-based application is to provide TTT job placement assistance in targeted local education agencies (LEAs). The Financial Management Information System (FMIS) application submits payment requests for various sources to the Defense Finance and Accounting Service (DFAS). The Warehouse Distribution System (WDS) application manages addresses, inventory and processes shipments of materials to DANTES customers. WDS allows authorized users to manage order limits for inventory items. External Interface - A file is produced and SFTPed to DFAS.

PII collected: Name, SSN (full and truncated), DoD ID number, Home Telephone Number, Personal Email Address, Mailing/Home Address, Financial and Employment Information: current employer, rank, pay grade; Education Information: highest level of education, transcripts, test scores. training courses taken, and certifications.

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

Privacy Risks in collection of data is reduced by the use of encryption, the risks of using privacy data are reduced by limiting data access, reduction of report displays to need to know information, tracking of hard copy reports from creation through destruction.
Participation in the DODVES Program is voluntary by the individual and users are notified before entering data our intent of adhering to the Privacy Act Laws.
The DODVES utilizes the defense-in-depth strategy to deploy security controls throughout the layers of the infrastructure to protect and preserve confidentiality. Identification and authentication (I&A) controls are in place to ensure users can only log in to the applications they need (and have permission) to, and can only access the data they are authorized to see. All users are required to use CAC logins to access the DODVES infrastructure. Each DODVES software application requires a username and password (whose construct complies with and exceeds the criteria stipulated in DON Policy). Only authorized, approved ports and protocols are opened to this host from the fire wall. The application server is not opened to the outside and folder/file access is limited to internal DANTES users only. Specific permissions are defined by each application's trusted facility management criteria. Any PII data that must remain on the DODVES infrastructure is protected by data-at-rest encryption. Any data transmitted to/ from the DODVES is encapsulated and protected by latest authorized encryption. All data contained in/attached to emails are encrypted and digitally signed by the DANTES sender. DODVES users complete IA and PIA training on an annual basis. The DODVES web application external users must complete and submit a SAAR-N, which validates their completion of IA training and their need to access the application.

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 SMART transcript service (now JST) via Navy College Management Information System (NCMIS)

☒ **Other DoD Components.**

Specify. DFAS, Community College of the Air Force (CCAF), Air Force's Automated Education Management System (AFAEMS), Army's Automated Education Management System (GoArmyEd), ACE Registry Transcript System and the Coast Guard Institute Transcript System.

☐ **Other Federal Agencies.**

Specify.

☒ **State and Local Agencies.**

Specify. Troops to Teachers State Representatives

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

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Prometric, ACT, GED Testing Service, Excelsior College,

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.

The following describes the scope for data consent for each of the applicable DODVES application modules. The individual may elect not to have their information collected, however this would mean they could not participate in the desired program. Participation is voluntary.

a. Troops to Teachers (TTT). The data utilized to provide TTT state offices and Local Education Agencies (school districts, schools etc) basic contact information about the TTT participants so that they can be evaluated and contacted for potential teaching positions as required by the No Child Left Behind Act. Also required is the SSN for any education reimbursements authorized by congress.
b. Jobs to Teach (J2T). The data is utilized to provide TTT state offices and Local Education Agencies (school districts, schools etc) basic contact information about the TTT participants so that they can be evaluated and contacted for potential teaching positions as required by the No Child Left Behind Act. Also required is the SSN for any bonus or stipends that they are entitled to receive under the TTT authorizations from congress.
c. DANTES Academic Information Management System (DAIMS). The DANTES Examination Program Handbook which is sited in the DoD Instruction 1322.25 as the guidelines for the management of the DANTES Examination Program specifies the requirement for the submission of the SSN by all military personnel nominated by their respective Service to serve as a DANTES Test Control Officer or Alternate Test Control Officer. If the military member objects to this requirement, DANTES will not appoint this individual.

Military examinees must sign a Privacy Release statement as a pre-condition for being authorized for a DANTES-funded test. The authority is 5 USC 301. If the individual refuses to sign this statement, they are

ineligible for DANTES-funded testing.

(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.

Military examinees must sign a Privacy Release statement as a pre-condition for being authorized. Any additional consent required due to special circumstances, the individual would be contacted.

(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: DOD Authorized Privacy Act Statements. On Web pages and Privacy Release statements for testing.

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.