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:

Department of Defense Voluntary Education System (DoDVES)

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

11/20/2018

Defense Activity For Non-Traditional Education Support (DANTES)

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.

Purpose of the system: To provide voluntary educational programs to current and former military service members. The system will maintain educational records and track educational costs of those current and former service members who participate in DANTES programs; assist military personnel in making successful transitions to second careers in teaching; provide referral assistance and placement services to separating, qualified, military personnel for K-12 schools that serve low-income families throughout the U.S.; provide information to the Defense Finance and Accounting Service (DFAS) and to DoD fiscal and accounting personnel for the purpose of financial management and funds disbursement; support the services' Tuition Assistance programs by managing Memoranda of Understanding with participating educational institutions; help prospective distance learners self-assess their readiness; and promote partnerships between civilian and military communities through agreements with commercial testing agencies, colleges, universities, and educational associations.

Types of PII information required to participate in our programs include data required to process financial records, records relating to service members' education, and identity verification. Specific PII collected include: Name, Social Security Number (SSN), DoD ID Number, employment information (teaching employment data, dates of employment, subjects/levels taught, district/school, certification/program licensure data, employment contract, title, department), home/cell phone, mailing/home address, work email address, military records (rank, service, service status, dates of service, separation data, enlistment/reserve contract), work/official duty address, work/official duty phone, rank/grade, race/ethnicity, date of birth, education information (degree, major/minor, grade point average, date of highest degree, institution, institution state, transcript), personal email address, and gender.

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)*

Missionsrelated use, verification, identification, and authentication of the user of the DODVES modules. Financial records require detailed identification of the individuals to ensure correct payments are made to the correct individuals. These same payments are reported for tax purposes to the IRS by DFAS. Score data records are provided to services transcript systems, who require PII to ensure correct identification of these academic records.

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.

The applications are used on a voluntary basis but are required to participate in the voluntary education programs. The individual has complete control of what information is entered.

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

The applications are used on a voluntary basis but are required to participate in the voluntary education programs. The individual has complete control of what information is entered.

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

DANTES Academic Information Management System (DAIMS) Exams Reimbursements

Authority: DoDI 1322.25, Voluntary Education Program; DoDD 1322.08E, Voluntary Education Programs for Military Personnel; and E.O.9397 (SSN), as amended.

Principal Purpose(s): To provide information to the Defense Finance and Accounting Service (DFAS) and to DoD fiscal and accounting personnel to authorize reimbursement of the GED, GRE General, GRE Subject, GMAT, Praxis Series, ACT and SAT exams administered at National and International Test Centers.

Routine Use(s): To the United States Coast Guard Voluntary Education Program Office for the purpose of education counseling, financial management, and funds disbursement. For a complete list of routine uses, visit the applicable system of records notice at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

Disclosure: Voluntary; however, failure to provide all required information on the form will complicate, delay, or possibly prevent the administrative actions necessary for reimbursement.

Troops to Teachers (TTT) Application
Authority: 10 U.S.C. 1154, Troops-to-Teachers Program; DoDI 1322.25, Voluntary Education Program; DoDD 1322.08E, Voluntary Education Programs for Military Personnel; and E.O.9397 (SSN), as amended.

Principal Purpose(s): To verify information provided relative to selection and to provide that information to school districts or institutions of higher education in order to provide referral assistance and placement services to separating, qualified military personnel.

Routine Use(s): To grant recipients at the state Departments of Education and their sub grantees to provide education transition services to current and former service members. For a complete list of routine uses, visit the applicable system of records notice at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

Disclosure: Voluntary; however, failure to provide the requested information may result in disqualification for participation or limited exposure to certification or employment opportunities.

Department of Defense Memorandum of Understanding (DoD MOU) Application
Authority: DoDI 1322.25, Voluntary Education Program; DoDD 1322.08E, Voluntary Education Programs for Military Personnel; and E.O.9397 (SSN), as amended.

Principal Purpose(s): To process memorandum of understanding applications and verify educational institution information provided is accurate and meets the DoDI 1322.25 eligibility requirements to participate in the military Tuition Assistance program.

Routine Use(s): To contractors responsible for performing or working on contracts for the DoD when necessary to accomplish an agency function related to this system of records. For a complete list of routine uses, visit the applicable system of records notice at: http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

Disclosure: Voluntary; however, failure to provide the requested information may result in a delay of processing and/or eligibility approval to participate in the military tuition assistance program.

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

☒ Within the DoD Component — Specify. Defense Logistics Agency (DLA), Defense Enrollment Eligibility Reporting System (DEERS), OUSD P&R

☒ Other DoD Components — Specify. U.S. Army, U.S. Air Force, U.S. Navy, Defense Finance & Accounting Service (DFAS)

[X] Other Federal Agencies	Specify.	US Coast Guard
[X] State and Local Agencies	Specify.	Grant recipients (Representatives from states Departments of Education)
[X] 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.	College Board, N0018917DZ050. FAR clauses: 52.224-1, Privacy Act Notification (APR 1984) 52.224-2, Privacy Act (APR 1984) 52.239-1, Privacy or Security Safeguards (AUG 1996) ACT Inc., N0018914DZ040. FAR clauses: 52.239-1, Privacy or Security Safeguards (AUG 1996) Prometric, N0018913DZ046. FAR clauses: 52.224-1, Privacy Act Notification (APR 1984) 52.224-2, Privacy Act (APR 1984) MCH Consulting Services, LLC, N0024416D0042. PWS 10.1 Privacy Act Compliance. The contractor may be in contact with data subject to the Privacy Act Title 5 of the U.S. Code, Section 552.a). The contractor shall ensure that employees assigned to this effort understand and adhere to the Privacy Act of 1974. The contractor shall identify and safeguard reports and data accordingly. The contractor shall follow DON policy and procedures detailed in SECNAVINST 5211.5D. The contractor shall ensure that contractor employees assigned to the contract are trained annually on properly identifying and handling Privacy Act data and information. The contractor shall furnish documentation evidencing such training to the Government upon request. N0018917QZ272, consolidated web support 16.1 Privacy Act. The contractor may be in contact with data subject to the Privacy Act Title 5 of the U.S. Code, Section 552.a). The contractor shall ensure that employees assigned to this effort understand and adhere to the Privacy Act of 1974. The contractor shall identify and safeguard reports and data accordingly. The contractor shall follow DoN Policy and procedures detailed in SECNAVINST 5211.5D. The contractor shall ensure that contractor employees assigned to the contract are trained annually on properly identifying and handling Privacy Act data and information. The contractor shall furnish documentation evidencing such training to the Government upon request.
[X] Other *(e.g., commercial providers, colleges)*.	Specify.	Universities, Educational Institutions

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

- [X] Individuals
- [X] Existing DoD Information Systems
- [X] Other Federal Information Systems
- [X] Databases
- [X] Commercial Systems

Defense Enrollment Eligibility Reporting System (DEERS), Veterans Affairs (VA), Department of Education Postsecondary Education Participants System (PEPS), educational institutions, grant recipients (and sub-grantees) at state Departments of Education, DoD contractors that administer exams (The College Board's internet-based testing platform, Prometric's internet-based testing platform, and ACT Inc's ACT Internet Reporting Option (AIRO)).

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

- [X] E-mail
- [X] Face-to-Face Contact
- [X] Official Form (*Enter Form Number(s) in the box below)*
- [X] Paper

[X] Fax
[X] Telephone Interview
[X] Information Sharing - System to System
[X] Website/E-Form
[ ] Other *(If Other, enter the information in the box below)*

DAIMS Reimbursements electronic form was approved as DANTES Form 1560/50
TTT Financial Eligibility School Verification online form - form request to be submitted
DoD MOU online form - form request to be submitted

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.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier DHRA19 DoD

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. Pending input

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

(3) Retention Instructions.

SF-115 with proposed records disposition submitted to NARA in June 2018. Records will be treated as permanent until records disposition schedule is approved by NARA.

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.

10 U.S.C. 1154, Troops-to-Teachers Program; DoDI 1322.25, Voluntary Education Program; DoDD 1322.08E, Voluntary Education Programs for Military Personnel; and 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 [X] 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.

Pending, Package submitted on 6 August 2018

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	

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.

SSN Justification Memo signed by NETC CIO dated 21 August 2012. New SSN Justification Memo submitted to DHRA CIO on 21 November 2017.

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

Computer matching is the primary use case that allows DODVES to uniquely track individuals who have not been issued a DoD ID number. Until that occurs, the only method to uniquely identify individuals and exchange information about them with external systems not transitioning to the DoD-ID is through the use of the SSN.

Legacy system is the secondary use case, similar to the primary case cited above. Many system interface partners may not be able to complete a transition away from the use of SSN as a unique primary identifier. For those systems, it may be necessary to continue to exchange data based on SSN even if an alternate identifier exists in DODVES.

(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".

Masking the display of SSN without a identifiable business need. Removal of SSN from all printed material.

(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

DFAS requires SSN to provide payments and collect federal income tax withholding. Military Services transcript systems and educational institutions require SSN for Computer Matching of student records.

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)*

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

Common Access Card (CAC) login. The SSC LANT, New Orleans Office is a gated area with one-way entrance and exit points, roaming patrols and closed circuits television coverage of sensitive areas. The entrance is guard or key card access controlled. An operator is on duty 24 hours a day, 7 days a week. All entries requiring key access are restricted to authorized personnel and are logged.

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

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

The Commanding Officer has designated server areas as Level Two Restricted Areas, and personnel authorized access must be on the access list for that area. All visiting personnel entering the area are required to sign a logbook and be escorted by authorized personnel.

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

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

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

Administrative: Access to the system is restricted to authorized personnel only using a Common Access Card (CAC). DODVES authorization is restricted to personnel with a demonstrated need-to-know, in the performance of their official duties. Risks of using privacy data are reduced by limiting data access, reduction of report displays to need-to-know information, and tracking of hard copy reports from creation through destruction.
Physical: Records are maintained within secured buildings in areas accessible only by properly trained and screened persons with an official need to know. Records are stored on secure military installations. Physical controls include use of visitor registers and identification badges, electronic key card access, and closed-circuit television monitoring. Backups are stored on encrypted media and secured off-site.
Technical: Technical controls including intrusion detection systems, secure socket layer encryption using DoD Public Key Infrastructure certificates, firewalls, and virtual private networks protect the data in transit and at rest. Usernames and passwords, Common Access Cards (CACs), and role-based access controls are used to control access to the systems data. Privacy Risks in collection of data is reduced by the use of encryption, and procedures are in place to deter and detect browsing and unauthorized access, including periodic security audits and monitoring of users' security practices. As new protections are developed, the hosting Data Center is proactive in applying IAVA, CTO, and STIG updates to stay within accepted compliance. The hosting Data Center uses an HBSS to protect the system, virus protection, malware protection, fire wall, spam protection, which is a defense-in-depth concept. The risk of unauthorized disclosure is low.