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:

National Security Education Program - Information Technology (NSEP-IT)

2. DOD COMPONENT NAME:	**3. PIA APPROVAL DATE:**
Defense Human Resources Activity	**10/30/2018**

Defense Language and National Security Education Office (DLNSEO)

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.

The NSEP-IT system is a comprehensive data collection system for tracking student progress within institutional academic programs, and recording federal service requirements. The system consists of three components: NSEPnet, the Student Certification System (SCS), and the NSEP Grants Database. Information is maintained in the SCS by the NSEP institutional academic programs for coding and tracking participating students in DoD funded educational programs. NSEPnet maintains records of all NSEP award recipients to track recipient progress towards fulfilling their service requirement. Data in the NSEP Grants Database is used to produce performance reporting metrics on institutions of higher education receiving NSEP institutional grant funding. These records are also used as a management tool for statistical analysis, tracking, reporting, and evaluating program effectiveness

The following information is collected from individual Scholarship/Fellowship recipients via the NSEPnet component of the NSEP-IT system: title; full name; current address, permanent address, Social Security Number (SSN), current telephone number, permanent telephone number, email address, voting district, date of birth, country or state of birth, citizenship status, educational information, region, country, and language to be studied under award, other languages spoken, proficiency in language studied at time of award, overseas experience, relevant activities, honors and awards, government agencies of interest, proposed study abroad program information and budget, other scholarship funding information, prior military service, gender, ethnicity, employer name and employer address, supervisor name, supervisor title, supervisor telephone number, position title, employment dates and hours, language used in position, security clearance held for position, award type, date of award completion, graduation date, length of service requirement, date of availability for work, information on veterans preference, Federal employment history, preferences with regard to being contacted by intelligence agencies, degree information, foreign language information, job search history, job history, overseas experience, other information (e.g., special recognitions or memberships, special skills and qualifications, fieldwork or volunteer experience, and foreign language(s) learned information).

For two of the NSEP institutional grant programs, The Language Flagship and Project Global Officer, the Student Certification System (SCS) collects the following participant information: full name; current address, permanent address, current telephone number, permanent telephone number, email address, date of birth, citizenship status, educational information, language of study, other languages spoken, proficiency in language, overseas study, scholarship funding information, prior military service, gender, family language use, and ethnicity.

The NSEP Grants Database does not collect PII.

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)*

NSEP-IT collects PII for verification and identification. All uses are mission-related uses, including authentication of the user for their access and tracking within the NSEP-IT systems. Social Security Numbers are only used for the identification of individuals to ensure repayment (when applicable) for non-compliance are sent to the U.S. Treasury for collection.

e. Do individuals have the opportunity to object to the collection of their PII?　☒ 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.

Individuals provide information voluntarily and are given the opportunity to object at time of data collection via a Privacy Act Statement.

f. 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.

NSEP awards including the English for Heritage Language scholarships, Boren Scholarships and Fellowships and Boren Flagship Scholarships that carry a service obligation require consent to use PII. Within the SCS system, all Language Flagship and ROTC Project GO students agree to the use of their data for the purposes of program tracking, monitoring and research. While consent is voluntary failure to furnish the requested information may result in ineligibility to receive an NSEP award.

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

The Privacy Act Statement provided for the on-line NSEPnet application reads:
Authority: 50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; 32 CFR 32.51, DoD Grant and Agreement Regulations (DoDGARs) Monitoring and Reporting Program Performance; DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) and NSEP Service Agreement; and E.O. 9397 (SSN), as amended..

Principle Purposes: To determine recipients of National Security Education Program awards.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

To Institutions of Higher Education who receive grant funding via The Language Flagship and Project Global Officer (Project GO) who use this for the monitoring and tracking of their own students participating in these programs

To the American Councils for International Education for the input of student proficiency scores for students assessed using their assessments.

To the Boren Forum, the non-profit NSEP alumni organization, to confirm the name, award year, and type of award of NSEP award recipients,

To consumer reporting agencies pursuant to guidance under 5 U.S.C. 552a(b)(12) as defined in the Fair Credit Reporting Act (14 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). Disclosure aids in the collection of outstanding debts owed the Federal Government.

The DoD Routine Use(s) can be found in the applicable system of records notice, DHRA 09, National Security Education Program Records, https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570561/dhra-09/

Disclosure: The completion of this form is voluntary. However, failure to furnish the requested information may result in ineligibility to receive an NSEP award.

The Privacy Act Statement printed on DD Form 2752 reads:
Authority: 50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; 32 CFR 32.51, DoD Grant and Agreement Regulations (DoDGARs) Monitoring and Reporting Program Performance; DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) and NSEP Service Agreement; and E.O. 9397 (SSN), as amended.

Principal Purpose(s): To establish a service agreement for all individuals receiving NSEP scholarships or fellowships.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended

To Institutions of Higher Education who receive grant funding via The Language Flagship and Project Global Officer (Project GO) who use this for the monitoring and tracking of their own students participating in these programs

To the American Councils for International Education for the input of student proficiency scores for students assessed using their

assessments.

To the Boren Forum, the non-profit NSEP alumni organization, to confirm the name, award year, and type of award of NSEP award recipients,

To consumer reporting agencies pursuant to guidance under 5 U.S.C. 552a(b)(12) as defined in the Fair Credit Reporting Act (14 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). Disclosure aids in the collection of outstanding debts owed the Federal Government.

The DoD Routine Use(s) can be found in the applicable system of records notice, DHRA 09, National Security Education Program Records, https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570561/dhra-09/

Disclosure: The completion of this form is voluntary. However, failure to provide information will result in NSEP not being able to finalize your application for a scholarship or fellowship. Social Security Number is requested to facilitate reporting to the Department of Treasury and the consumer reporting agencies in the event of default.

The Privacy Act Statement on DD Form 2753 reads:
Authority: 50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; 32 CFR 32.51, DoD Grant and Agreement Regulations (DoDGARs) Monitoring and Reporting Program Performance; DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) and NSEP Service Agreement; and E.O. 9397 (SSN), as amended.

Principal Purpose(s): To document recipient's status and compliance in fulfilling the service requirement.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

To Institutions of Higher Education who receive grant funding via The Language Flagship and Project Global Officer (Project GO) who use this for the monitoring and tracking of their own students participating in these programs

To the American Councils for International Education for the input of student proficiency scores for students assessed using their assessments.

To the Boren Forum, the non-profit NSEP alumni organization, to confirm the name, award year, and type of award of NSEP award recipients,

To consumer reporting agencies pursuant to guidance under 5 U.S.C. 552a(b)(12) as defined in the Fair Credit Reporting Act (14 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). Disclosure aids in the collection of outstanding debts owed the Federal Government.

The DoD Routine Use(s) can be found in the applicable system of records notice, DHRA 09, National Security Education Program Records, https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570561/dhra-09/

Disclosure: Voluntary; however, failure to furnish the requested information may result in your being required to reimburse the U.S. Treasury for the total cost of your scholarship or fellowship plus interest. A truncated SSN (last four digits of your Social Security Number) is requested in order to track award recipients in the case that their name and/or address changes.

The Privacy Act Statement provided for Student Certification System and Grant Performance Report applications reads:

Authority: 50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; 32 CFR 32.51, DoD Grant and Agreement Regulations (DoDGARs) Monitoring and Reporting Program Performance; DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) and NSEP Service Agreement; and E.O. 9397 (SSN), as amended.

Principle Purposes: To determine recipients of National Security Education Program awards.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. The DoD Routine Use(s) can be found in the applicable system of records notice, DHRA 09, National Security Education Program Records, https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570561/dhra-09/

Disclosure: Voluntary; however, failure to furnish the requested information results in ineligibility to receive an NSEP awards.

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

[X] Within the DoD Component   Specify.   Information will be used by NSEP personnel who require the records in the performance of their official duties.

[X] Other DoD Components   Specify.   Authorized DoD hiring officials, to facilitate the recruiting of NSEP award recipients into federal service for the purpose of fulfilling NSEP's mission.

[X] Other Federal Agencies   Specify.   Individuals who are non-compliant with Service Agreement and who fail to pay back awards are sent to the U.S. Treasury for collection.

[ ] State and Local Agencies   Specify.

[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.   The prime contractor charged with hosting and data safeguarding is Advanced Software Systems, Inc. (ASSYST), which is required to meet DoD IRisk Management Framework (RMF) standards in accordance with DoDI 8510.01. The contractor routine use is listed in the SORN. The 52.224-1 Privacy Act Notification 52.224-2 Privacy Act 52.224-1 are included in active contract.

[X] Other *(e.g., commercial providers, colleges).*   Specify.   To Institutions of Higher Education who receive grant funding via The Language Flagship and Project Global Officer (Project GO) who use this for the monitoring and tracking of their own students participating in these programs.

To The Institute for International Education for monitoring the performance of The Language Flagship and Project GO institutional programs and student performance in these programs, also review and validation of NSEP awardee information and repayments.

To The American Councils for International Education for the input of student proficiency scores for students assessed using their assessments.

To The Boren Forum, the non-profit NSEP alumni organization, to confirm the name, award year, and type of award of NSEP award recipients to consumer reporting agencies.

To consumer reporting agencies pursuant to guidance under 5 U.S.C. 552a(b)(12) as defined in the Fair Credit Reporting Act (14 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). Disclosure aids in the collection of outstanding debts owed the Federal Government. Disclosure is limited to name, address, and taxpayer identification number (SSN); the amount, status, and history of the claim; and the agency or program under which the claim arose.

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

[X] Individuals   [ ] Databases

[ ] Existing DoD Information Systems   [ ] Commercial Systems

[ ] Other Federal Information Systems

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

☐ E-mail	☐ Official Form *(Enter Form Number(s) in the box below)*
☐ Face-to-Face Contact	☐ Paper
☐ Fax	☐ Telephone Interview
☐ Information Sharing - System to System	☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*	

DD 2752, NSEP Service Agreement Report (SAR) for Scholarship and Fellowship Awards
DD 2753, NSEP Service Agreement for Scholarship and Fellowship Awards

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 <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☒ Yes   ☐ No

If "Yes," enter SORN System Identifier | DHRA 09 |

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. | N1-330-13-03 and GRS 1.2, Item 020 |

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

(3) Retention Instructions.

Unsuccessful NSEP student award applications- Destroy after 5 years (N1-330-13-03)

Successful institutional grant reports- Destroy after 10 years (GRS 1.2, Item 020)

Records of language acquisition progress among students; successful NSEP student award applications; and records of service requirement fulfillment among NSEP student award recipients - Destroy after 30 years (N1-330-13-03)

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.

50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; 32 CFR 32.51 DoD Grant and Agreement Regulations

(DoDGARs) Monitoring and Reporting Program Performance; DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) and NSEP Service Agreement; 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   ☐ 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.

OMB Number 0704-0368, National Security Education Program (NSEP) Service Agreement Report for Scholarship and Fellowship Awards, August 17, 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		

Voting district, region, country, and language to be studied under award, other languages spoken, proficiency in language studied at time of award, overseas experience, relevant activities, honors and awards, government agencies of interest, proposed study abroad program information and budget, other scholarship funding information, award type, date of award completion, length of service requirement, date of availability for work, preferences with regard to being contacted by intelligence agencies, foreign language information, overseas experience, family language uses, and other information (e.g., special recognitions or memberships, special skills and qualifications, fieldwork or volunteer experience, and foreign language(s) learned information).

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.

12/12/2018

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

Computer matching

(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".

Access to and use of SSN is limited to DLNSEO Service Team staff. SSNs have been removed from all printed material and non-NSEP-IT electronic media

(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

DLNSEO requires SSNs for the limited number of delinquent accounts to identify those awardees who are required to pay back their awards. This information is used by the U.S. Treasury for the collection of delinquent awardee repayments.

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.

c. How will the PII be secured?

(1) Physical Controls. *(Check all that apply)*

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

Physical/ digital access to records is restricted to those who require the data in the performance of their official duties. PhThe NSEP-IT system has all data storage at an off-site facility that meets DoD and National Institute Standard of Technology (NIST) requirements for data security.

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

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

Additionally, contract officers are required to incorporate all appropriate Privacy Act clauses and contractor personnel are required to sign nondisclosure documents holding them to all provisions of the Privacy Act.

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

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

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

As new protections are developed, the hosting Data Center is proactive in applying IAVA, CTO, and STIG updates to stay within accepted compliance. Privacy risks in collection of data are 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, and tracking of hard copy reports from creation through destruction. The Data Center hosting the system utilizes a HBSS to protect the system, virus protection, malware protection, fire wall, and spam protection, which is a defense in depth concept. The risk of unauthorized disclosure is low.