PRIVACY IMPACT ASSESSMENT (PIA)

For the

National Security Education Program Information Technology (NSEP-IT)

National Security Education Program (NSEP), Defense Language and National Security Education Office (DLNSEO)\Defense Human Resources Activities (DHRA), Undersecretar

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: 14164
- ☐ **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 000006726

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 DHRA 09

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 0704-0368

Enter Expiration Date 11/30/2017

☐ **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.

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, 5 CFR 1320, Controlling Paperwork Burdens on the Public, DoD Instruction (DoDI) 1025.02, National Security Education Program (NSEP) And NSEP Service Agreement; and 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.

To accomplish this mission, NSEP awards funding to students in the forms of Boren Scholarships, Boren Fellowships, Flagship Fellowships, English for Heritage Language Speakers (EHLS) Scholarships for foreign language study. These awards are collectively referred to as NSEP student awards. In exchange for these awards, recipients incur a legislatively-mandated service requirement. Additionally, NSEP awards grants to academic institutions that allow those institutions to establish intensive foreign language programs. In exchange for these grants, institutions must report student progress in foreign language acquisition.

NSEP-IT systems include NSEPnet, the Student Certification System (SCS) and the NSEP Grants Database. NSEPnet and SCS capture data related to U.S. undergraduate and graduate students receiving funding through NSEP programs, the NSEP Grants Database captures performance reporting from institutions of higher education receiving NSEP institutional grant funding.

Information collected on individuals via the NSEP-IT systems includes: title; full name; current address, city, state, and zip code; permanent address, city, state; Social Security Number (SSN); current telephone number and permanent telephone number; email address; voting district; date of birth; country or state of birth; naturalization information; 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, title, and 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, and preferences with regard to being contacted by intelligence agencies; degree information; foreign language information; job history; overseas experience; other information e.g., special recognitions or memberships; special skills and qualifications; fieldwork or volunteer experience; nationality; foreign language(s) learned information, which includes any educational.

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

PRIVACY RISKS (Collection, Use, and Sharing): Access, storage and transmission of information protected under the Privacy Act of 1974 are subject to threats, including, but not limited to: malware, sniffing, spoofing, and physical assault, as well as various natural disasters and failures which impact either the protected infrastructure or the services upon which the infrastructure depends. All of these imperil, to one extent or another, information availability, integrity, and confidentiality.

NSEP reviewed the safeguards established for the system to ensure they are compliant with DOD cybersecurity and data storage requirements and are appropriate to the sensitivity of the information stored within the system. Any specific routine uses have been reviewed to ensure the minimum amount of personally identifiable information is provided. Physical/digital access to records is restricted to those who require the data in the performance of their official duties. Physical entry to data servers is restricted by the use of locks, guards, and administrative procedures. The NSEP-IT system has all data storage at an off-site facility that meets DOD and NIST requirements for data security. The facility requires identification badges to access the system. The government offices where system data is accessed by federal personnel requires key card entry. Access to information for federal users is further restricted by using Common Access Card (CAC) and PIN to access the computer system and program passwords that are changed every 180 days to access system and online databases. The following technical controls are also applied to restrict access to those who require the data in the performance of their official duties: intrusion detection system; encryption; external Certificate Authority (CA) certificate; firewall; and, DoD Public Key Infrastructure (PKI) certificates. PII is encrypted when transmitted electronically.

The following administrative controls are also applied to restrict access to those who require the data in the

performance of their official duties: periodic security audits; regular monitoring of users' security practices; methods to ensure only authorized personnel have access to Personally Identifiable Information (PII); encryption of backups containing sensitive data. Additionally, contract officers are required to incorporate all appropriate Privacy Act clauses in their contracts, and contractor personnel are required to sign nondisclosure documents holding them to all provisions of the Privacy Act.

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. Information will be used by NSEP personnel who require the records in the performance of their official duties.

☒ **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.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

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

Specify. The prime contractor charged with hosting and data safeguarding is Advanced Software Systems, Inc. (ASSYST), which is required to meet DoD Information Assurance Certification and Accreditation Process (DIACAP) standards in accordance with DoDI 8510.01. The contractor routine use is listed in the SORN.

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

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

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.

Voluntary; however, failure to furnish the requested information may result in ineligibility to receive an NSEP award.

(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.

NSEP awards including The Language Flagship student support, Project GO student support, as well as the English for Heritage Language scholarships, Boren Scholarships and Fellowships that carry a service obligation. NSEP requires all elements named above in order to ensure the eligibility for award. Data are also used to target student outreach and recruitment, and monitor retention and completion. Most importantly, NSEP must track and maintain up to date records on individual recipients to ensure compliance with the legislatively-mandated service obligation. Within the SCS system, students agree to the use of their data for the purposes of program tracking, monitoring and research. For the EHLS and Boren programs NSEP requires all elements named above in order to, first, award the most competitive applicants.

(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.

The Privacy Act Statement provided for the online application reads:

Authority: 50 U.S.C. 1901, David L. Boren National Security Education Act of 1991; DoD Instruction (DoDI) 1025.02, National Security Education Program; DoDI 1025.6, National Security Education Program (NSEP) Service Agreement; and E.O. 9397 (SSN), as amended.

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

applicable System of Records Notice is DHRA 09 National Security Education Program - Information Technology (NSEP-IT) System located at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570561/dhra-09/

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

Applicable Blanket Routine Use(s) are: a) Law Enforcement Routine Use, b).Congressional Inquiries Disclosure Routine Use, c) Department of Justice for Litigation Routine Use, d) Disclosure of Information to the National Archives and Records Administration Routine Use, and e) Data Breach Remediation Purposes Routine Use. The complete list of DoD Blanket Routine Uses can be found online at http://dpcld.defense.gov/Privacy/SORNsIndex/Blanket-Routine-Uses/.

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., Chapter 37, the David L. Boren National Security Education Act of 1991; DoD Instruction (DoDI) 1025.02, National Security Education Program; DoDI 1025.6, National Security Education Program (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. The applicable System of Records Notice is DHRA 09 National Security Education Program - Information Technology (NSEP-IT) System located at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570561/dhra-09/

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

Applicable Blanket Routine Use(s) are: a) Law Enforcement Routine Use, b).Congressional Inquiries Disclosure Routine Use, c) Department of Justice for Litigation Routine Use, d) Disclosure of Information to the National Archives and Records Administration Routine Use, and e) Data Breach Remediation Purposes Routine Use. The complete list of DoD Blanket Routine Uses can be found online at http://dpcld.defense.gov/Privacy/SORNsIndex/Blanket-Routine-Uses/.

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:

uthority: 50 U.S.C., Chapter 37, the David L. Boren National Security Education Act of 1991; DoD Instruction (DoDI) 1025.02, National Security Education Program; DoDI 1025.6, National Security Education Program (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. TThe applicable System of Records Notice is DHRA 09 National Security Education Program - Information Technology (NSEP-IT) System located at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570561/dhra-09/

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

Applicable Blanket Routine Use(s) are: a) Law Enforcement Routine Use, b).Congressional Inquiries Disclosure Routine Use, c) Department of Justice for Litigation Routine Use, d) Disclosure of Information to the National Archives and Records Administration Routine Use, and e) Data Breach

Remediation Purposes Routine Use. The complete list of DoD Blanket Routine Uses can be found online at http://dpcld.defense.gov/Privacy/SORNsIndex/Blanket-Routine-Uses/.

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 Grantapplications reads:

Authority: 50 U.S.C., Chapter 37, the David L. Boren National Security Education Act of 1991; DoD Instruction (DoDI) 1025.02, National Security Education Program; DoDI 1025.6, National Security Education Program (NSEP) Service Agreement; and E.O. 9397 (SSN), as amended.
Principle Purposes: To determine recipients of National Security Education Program awards.

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

Applicable Blanket Routine Use(s) are: a) Law Enforcement Routine Use, b).Congressional Inquiries Disclosure Routine Use, c) Department of Justice for Litigation Routine Use, d) Disclosure of Information to the National Archives and Records Administration Routine Use, and e) Data Breach Remediation Purposes Routine Use. The complete list of DoD Blanket Routine Uses can be found online at http://dpcld.defense.gov/Privacy/SORNsIndex/Blanket-Routine-Uses/.

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

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.