SYSTEM NAME AND NUMBER: National Security Education Program – Information Technology (NSEP-IT) System, DHRA 09. (April 3, 2020; 85 FR 18926)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Amazon Web Services (AWS), US West, Astoria, OR 97103.

Institute of International Education, 1400 K Street NW, Suite 650, Washington, DC 20005-2403.

SYSTEM MANAGER(S): Program Manager, Defense Language and National Security Education Office, National Security Education Program, 4800 Mark Center Drive, Suite 08G08, Alexandria, VA 22350-1500, nsep@nsep.gov, 571-256-0702.

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

PURPOSE(S) OF 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. NSEP Grants Database data is used to produce performance reporting metrics on institutions of higher education receiving NSEP institutional grant funding. Also, these records are used as a management tool for statistical analysis, tracking, reporting, and evaluating program effectiveness.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals applying for and receiving David L. Boren Scholarships, English for Heritage Language Speakers (EHLS) Scholarships, David L. Boren Fellowships, and Flagship Fellowships; Individual students participating in university programs with NSEP-funded grants for implementing “The Language Flagship” or “Project Global Officer” language training programs.

CATEGORIES OF RECORDS IN THE SYSTEM: Individual Scholarship/Fellowship recipients' title, full name, current address, permanent address, Social Security Number (SSN), current telephone number, permanent telephone number, email address, date of birth, country or state of birth, citizenship status, education, region, country, and, prior military service, gender, race/ethnicity, position title, 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. For two of the NSEP institutional grant programs, The Language Flagship and Project Global Officer and the Student Certification System (SCS) collect the following participant information: full name, current address, permanent address, current telephone number, permanent telephone number, email address, date of birth, citizenship status, prior military service, gender, and race/ethnicity.

RECORD SOURCE CATEGORIES: Individuals, and academic institutions.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, these records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. 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.

b. 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, as well as reviewing and validating NSEP awardee information and repayments.

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

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

e. 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 to 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.

f. To the U.S. Department of Treasury (Treasury) for individuals not compliant with the Service Agreement and who fail to pay back awards. Their name, address, and taxpayer identification number/SSN including the amount, status, and history of the claim are sent to the Treasury for collection.

g. To authorized federal hiring officials for the purpose of recruiting of NSEP award recipients into federal service, and assisting NSEP award recipients in fulfilling their Congressionally-mandated service requirement.

h. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this System of Records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure that apply to DoD officers and employees.

i. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

j. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

k. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

l. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

m. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

n. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the System of Records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

o. To another Federal agency or Federal entity, when the DoD determines information from this System of Records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by last name, first name, institution, and language.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Unsuccessful NSEP student award applications—Destroy after 5 years.

Successful institutional grant reports—Destroy after 10 years.

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.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Physical/digital access to records is restricted to those requiring the data in the performance of their official

duties. Physical entry to data servers is restricted by locks, guards, and administrative procedures. The NSEP-IT system maintains all data storage at an off-site facility, which meets all DoD and National Institute Standard of Technology requirements for data security. The facility requires identification badges for access. Additionally, access to system data requires a Common Access Card and a personal identification number. In addition, system entry requires that program passwords be changed every 180 days.

The following technical controls restrict access to those requiring the data in the performance of their official duties: Intrusion detection system; encryption; external Certificate Authority certificate; firewall; and, DoD Public Key Infrastructure certificates. Personally Identifiable Information (PII) is encrypted when transmitted electronically. Administrative controls restrict access to those requiring the data in the performance of their official duties or for reporting purposes: Periodic security audits; regular monitoring of users' security practices; methods to ensure only authorized personnel may access PII; encryption of backups containing sensitive data. Additionally, contract officers must follow all appropriate Privacy Act clauses. Also, contractor personnel must sign nondisclosure documents certifying their adherence to the provisions of the Privacy Act.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed written requests should contain full name, SSN, current address and telephone number of the individual, and the name and number of this SORN. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to NSEP-IT, Defense Language and National Security Education Office (DLNSEO), 4800 Mark Center Drive, Suite 08G08, Alexandria, VA 22350-1500. Signed written requests should contain full name, SSN, current address and telephone number of the individual, and the name and number of this SORN. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 79 FR 19585, April 09, 2014.