SYSTEM NAME AND NUMBER: Science, Mathematics, and Research for Transformation (SMART) Information Management System, DUSDA 14. (October 29, 2020; 85 FR 68567)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Logistics Management Institute (LMI), Ashburn Data Center, Ashburn, VA 20147-6011.

LMI San Antonio Office, 1777 NE Interstate 410 Loop #808, San Antonio, TX 78217-0000.

LMI Tyson's Office, 7940 Jones Branch Drive, Tysons, VA 22102-3381.

Scholarship America, One Scholarship Way, St. Peter, MN 56082-1693.

Mark Center, 4800 Mark Center Drive, Alexandria, VA 22350-1700.

SYSTEM MANAGER(S): Program Manager, SMART Scholarship for Service Program, 4800 Mark Center Drive, Alexandria, VA 22350-3600. OSD.SMART@mail.mil, 571-372-6535.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 3304, Competitive Service, Examinations; 10 U.S.C. 2192a, Science, Mathematics, and Research for Transformation (SMART) Defense Education Program; 20 U.S.C. 17, National Defense Education Program; DoD Instruction 1400.25, Volume 410, DoD Civilian Personnel Management System: Training, Education, and Professional Development; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: To enable SMART officials to select qualified applicants, to award SMART scholarships, and monitor participant progress and status through the program. Also, the system is used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Applicants and participants of the SMART Scholarship for Service Program.

CATEGORIES OF RECORDS IN THE SYSTEM: Information includes full name and any other names used, Social Security Number (SSN), home and school mailing addresses, home and cell phone numbers, school and alternate email addresses.

Additional information collected may include SMART Program identification number, resumes and/or curricula vitae, publications, citizenship status, Selective Service registration status, birth date, employment status, state and country of birth, race/ethnicity, gender, security clearance status, veterans preference, academic status, assessment test scores, copies of transcripts, bank account numbers, Individualized Education Program (IEP) or special accommodation testing requirements, projected and actual graduation dates, and projected and actual award amounts.

RECORD SOURCE CATEGORIES: The SMART Program manages individual source records using the SMART Information Management System (SIMS). The SIMS collects the following information and forms to confirm scholar compliance: Applicant transcripts, educational work plan and declaration of Federal Employment (OF-306). In addition, the SIMS uses a form (application) to collect eligibility information. The applicants report citizenship status, if they are 18 years of age, their proposed degree completion date, their proposed STEM discipline, and whether they are willing to complete an internship period and an employment period. The SIMS tracks individual compliance and non-compliance using a data table and trackers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE 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, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to § 552a(b)(3) as follows:

a. 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.

b. To academic institutions for the purpose of providing progress reports for applicants and participants.

c. To consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)). The purpose of this disclosure is to aid in the collection of outstanding debts owed to the Federal government, typically to provide an incentive for debtors to repay delinquent Federal government debts by making these debts part of their credit records.

d. 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.

e. 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.

f. 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 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.

g. 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.

h. 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.

i. 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.

j. 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: Paper and electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name and SMART Program identification number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Participant information. Delete/Destroy 6 years and 3 months after completion of service commitment, or upon repayment of funds. Records of individuals not chosen for participation in the program. Delete 3 years after final decision. DoD research and engineering facility data. Delete/Destroy upon termination of affiliation.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Access to records is permission-granted based on the role of the individual (need-to-know) and further restricted to individuals who require the data in the performance of official duties. Electronic records are maintained on servers in controlled areas accessible only to authorized personnel. Access to storage areas is restricted to personnel with a valid requirement and authorization to enter. Hardcopy records are kept in locked safes. Physical entry is restricted by the use of one or more of the following: security guards, identification badges, cipher locks, electronic locks, combination locks, key card access and closed circuit TV. Technical controls consist of user identification, passwords, intrusion detection systems, encryption, External Certificate Authority, firewalls, Virtual Private Network (VPN), DoD Public Key Infrastructure certificates, and Common Access Cards (CACs). Administrative controls consist of periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel have access to Personally Identifiable Information (PII), and personnel with access to SMART PII completing annual Information Assurance and Privacy Act training, as required by the DoD.

RECORD ACCESS PROCEDURES: Individuals seeking access to information 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, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed, written requests should contain the individual's full name and SMART Program identification number, and the name and number of this system of records notice. 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, for contesting contents and appealing initial agency determinations are published in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether this system of records contains information about themselves may address their inquiries to the Director, SMART Scholarship for Service Program, 4800 Mark Center Drive, Alexandria, VA 22350-3600. Signed, written requests should contain the individual's full name and SMART Program identification number. 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: October 20, 2016, 81 FR 72577.