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:

Science, Mathematics, and Research for Transformation (SMART) Scholarship-for-Service Program, Defense Education Program

2. DOD COMPONENT NAME:

If Other, enter the Component name in the box below.

Office of the Under Secretary of Defense for Research and Engineering

3. PIA APPROVAL DATE:

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)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] 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 purpose of this DoD information system is to enable SMART officials to select qualified applicants to be awarded SMART scholarships and monitor scholar progress and status through the program. The system is also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research. Information stored about SMART applicants and scholars include full name and any other names used, Social Security Number (SSN) (including truncated versions of the SSN), home and mailing addresses; home and cell phone numbers; and school and alternate e-mail addresses.

Additional information collected in the system includes SMART Program identification number, resumes and/ or curricula vita, publications, U.S. Citizenship, Selective Service registration status, birth date, employment status, state and country of birth; employment status, race/ ethnicity (optional), gender, veterans preference, information on academic background. and program information such as academic status, assessment test scores, copies of transcripts, financial and disability information, projected and actual graduation dates, service commitment start and end dates and projected and actual award amounts.

SMART Program support staff enters other program information unique to each scholar that includes projected and actual service commitment start and end dates, projected and actual award amounts, and security clearance status.

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)*

As required by the government, the SMART service agreement includes a field for the Scholar's SSN because if a SMART Scholar does not fulfill their service commitment to the DoD, the SSN is a requirement for the government in order to initiate debt collection; therefore, it is necessary that the SSN number be provided. Additionaly, by the Internal Revenue Service (IRS), the SSN is used as an identity credential pursuant to regulations since some of the monies provided to the participants is considered taxable income and therefore, must be reported to the IRS by providing scholars an IRS Form 1099-MISC. The SSN is a required field on the MISC-1099. Therefore, it is necessary that the SSN be provided.

e. Do individuals have the opportunity to object to the collection of their PII? [ ] Yes [x] 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 SMART Program Office requires an applicant's PII to evaluate application and award SMART scholarships. The Privacy Act Statement on the SMART application portal contains the following verbiage:

AUTHORITY: 10 U.S.C. 2192a, as amended; P.L. 109-163; and E.O. 9397 (SSN), as amended.
PRINCIPAL PURPOSES: To evaluate a SMART Applicant's qualifications for a SMART Scholarship

ROUTINE USE(S): A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.
DISCLOSURE: Failure to furnish the requested information on this form will result in SMART Participant not being non-compliant with SMART policy and subject to possible dismissal.

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.

The SMART Scholarship Program Privacy Act Statement must be signed by all applicants to whom scholarship awards have been offered. There is also a "Media Release" which grants SMART and/or its agents, employees, licensees and/or assignees permission to use, exploit, adapt, modify, reproduce, distribute, publicly perform and/or display, in any form now known or later developed, my image or visual likeness, my name, my voice, and information related to my experience with SMART

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

A Privacy Act Statement is provided when an applicant accesses the SMART application instructions via the SMART application portal managed by Logistics Management Institute (LMI), current cooperative agreement holder. The statement reads as follows: "AUTHORITY: 10 U.S.C. 2192a, as amended; P.L. 109-163; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSES: To evaluate a SMART Applicant's qualifications for a SMART Scholarship

ROUTINE USE(S): A record from a system of records maintained by a DoD Component may be disclosed as a routine use to a federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a DoD Component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

DISCLOSURE: Failure to furnish the requested information on this form will result in SMART Participant not being non-compliant with SMART policy and subject to possible dismissal.

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.	Army, Naval, and Air Force Sponsoring Facilities
☒	Other DoD Components	Specify.	Other DoD Sponsoring Facilities
☐	Other Federal Agencies	Specify.	
☐	State and Local Agencies	Specify.	
☐	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.	
☐	Other *(e.g., commercial providers, colleges).*	Specify.	

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

☒ 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

[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)*

DD784-1 thru DD784-15

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 DUSDA14

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.

It has been previously published but it is due to expire in July. We are currently working on new SORN as well

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. NI-330-09-3

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

(3) Retention Instructions.

Temporary: Participant information will be deleted/ destroyed 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 will be deleted when 3 years old. DoD sponsoring facilities will delete/ destroy upon termination of affiliation.

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.

5 U.S.C. 3304, Competitive Service, et seq.: 20 U.S.C. 17, National Defense Education Program, as amended
10 U.S.C. 2192a, Science, Mathematics, and Research for Transformation (SMART) Defense Education Program
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.

[X] 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 O7O4-O466

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	

5400.11.r

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.

The last signed memo was dated February 26, 2016. A new memo has been created and will be signed by Dr. Jagadeesh Pamulapati, Director, Laboratories Office

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

The justification for the use of the Social Security Number (SSN) is for financial and reporting reasons as required by the Department of Treasury. Through a cooperative agreement funded by the DoD, the Logistics Management Institute (LMI) provides SMART Scholarship participants with monthly stipend payments as well as book allowance, a medical allowance, and associated education fees. Tuition payments are made by LMI on behalf of the participants directly to the academic institution

(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".

The SMART Information Management System (SIMS) houses data on SMART scholars by classifying each scholar by a unique identifier code (UIC) to separate the personal identifiable information (PII) as identification credential source. This avoids unnecessary use of SSNs. Additionally, records visible to scholars have the SSNs redacted from the files that are maintained for archival purposes. Redaction of SSNs from stagnant archival records protects the sensitive data that is housed in the scholar portal.

(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

SMART cannot eliminate the use of SSN's as it is required for tax and other financial purposes along with clearance investigations. However, SSNs are not visible in the SIMS database as they are masked by the SMART ID.

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

Key locks

(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
- [ ] Regular Monitoring of Users' Security Practices
- [ ] If Other, enter the information in the box below

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

- [ ] Biometrics
- [x] Common Access Card (CAC)
- [x] DoD Public Key Infrastructure Certificates
- [x] Encryption of Data at Rest
- [x] Encryption of Data in Transit
- [x] External Certificate Authority Certificates
- [x] Firewall
- [ ] Intrusion Detection System (IDS)
- [ ] Least Privilege Access
- [x] Role-Based Access Controls
- [x] Used Only for Privileged (Elevated Roles)
- [x] User Identification and Password
- [x] 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?