PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

DoD Information Assurance Scholarship Program (IASP)

DoD Component Name:

National Security Agency

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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) 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. NSA/CSS Information Systems use the Intelligence Community IT Registry in lieu of the DITPR.

c. If "Yes," then a PIA is required. Proceed to Section 2.

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20340701

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:

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:

☒ **No**

☐ **Not Applicable**

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** **Enter UPI:**

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

☒ **No**

☐ **Not Applicable**

d. Does the DoD information system or electronic collection have 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** **Enter Privacy Act SORN Identifier:** GNSA 27

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

☐ **No** **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: 0704-0486

Enter Expiration Date: 02/28/2013

☐ **No**

☐ **Not Applicable**

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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.

a. (U) Sections 2200 et seq. and 7045 of title 10, United States Code
b. (U) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise." February 10, 2009
c. (U) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
d. (U) DoD Instruction 5025.01, "DoD Directives Program," October 28, 2007
e. (U) Deputy Secretary of Defense Memorandum, "Delegation of Authority and Assignment of Responsibility under Section 992 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001," June 26, 2001
f. (U) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
g. (U) Assistant Secretary of Defense for Command, Control, Communications and Intelligence Memorandum, "Information Assurance Scholarship Program," July 25, 2001 (hereby cancelled)
h. (U) DoD 8910.1-M, "Department of Defense Procedures for Management of Information Requirements," June 30, 1998
i. (U) DoD Instruction 5105.18, "DoD Intergovernmental and Intragovernmental Committee Management Program," July 10, 2009
j. (U) DoD 7000.14-R, Volume 5, Chapter 28, "Department of Defense Financial Management Regulation (FMR)," February 2010
k. (U) Section 303a(e) of title 37, United States Code

l. (U) Section 213.3102(r) of title 5, Code of Federal Regulations
m. (U) Under Secretary of Defense for Personnel and Readiness Memorandum, "Implementation Authority to Employ Individuals Completing Department of Defense Scholarship or Fellow Programs," April 5, 2010
n. (U) Section 1001 of title 20, United States Code
o. (U) Section 11101 of title 40, United States Code
p. (U) DoD 8145.01, "DoD Information Assurance Scholarship Program," January 17, 2012

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.

(U) The Information Assurance Scholarship Program (IASP), authorized by Section 2200 of title 10 of the United States Code is designed to: increase the number of new entrants to DoD who possess key Information Assurance (IA), Information Technology (IT) and Cybersecurity skill sets, and serve as a tool to develop and retain well-educated military and civilian personnel who support the Department's critical IT management and infrastructure protection functions.

(U) The recruitment and retention portions of the scholarship require a competitive application process. This application requires individuals to provide PII.

(U) The IASP recruitment is for college students who, on completion of the program, come to work for the DoD. The following information is collected from recruitment applicants:
Full Name
Mailing/Home Address
Personal Cell Telephone Number
Home Telephone Number
Personal Email Address
Employment Information
Military Records
Education Information

(U) The IASP retention is for current DoD civilians and active duty military members who return to school to complete a graduate degree. Upon completion of the program, the DoD employees return to their parent organization. The following information is collected from retention applicants:
Full Name
Mailing/Home Address
Personal Cell Telephone Number
Home Telephone Number
Personal Email Address
Unclassified Work Email Address
Employment Information
Military Records
Education Records
Security Clearance Information

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

(U) Should PII that is collected be unintentionally released, advisories would have access to location (address, phone numbers), education background, prior employment history, clearance level and in very rare cases social security numbers. Appropriate safeguards are in place for the collection, use, and sharing of information. Security measures are adequate and risk is minimal. Information is protected by user login/passwords and antivirus software. When information is shared with other authorized users, appropriate measures are in place to safely transmit / transport that information. This is done through digitally signed emails and certified mail couriers.

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

(U) DoD IASP Program Office/Team (I084);
I, Information Assurance Directorate;
I08, Workforce Resources, Education and Development;
I082, Intern Development;
ADET, Associate Directorate for Education and Training;
M, Associate Directorate for Human Resources;
MB, Office of Recruitment;
MR, Employee Relations

☒ **Other DoD Components.** Specify

(U) Department of the Navy;
Department of the Air Force;
Department of the Army;
Defense Advanced Research Projects Agency;
Defense Commissary Agency;
Defense Contract Audit Agency;
Defense Contract Management Agency;
Defense Finance and Accounting Service;
Defense Information Systems Agency;
Defense Intelligence Agency;
Defense Manpower Data Center;
Defense Media Activity;
Defense Logistics Agency;
Defense Technical Information Center;
Defense Threat Reduction Agency;
Missile Defense Agency;
National Geospatial-Intelligence Agency;
National Guard Bureau;
National Reconnaissance Office;
TRICARE Management Activity;
Washington Headquarters Service;
Pentagon Force Protection Agency;

☐ **Other Federal Agencies.** Specify

☐ **State and Local Agencies.** Specify

☐ **Contractor** (enter name and describe the language in the contract that safeguards PII.) Specify

☐ **Other** (e.g., commercial providers, colleges). Specify

i. 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.

(U) The information is requested from the applicant when he/she applies for the scholarship program. The Privacy Act statement used for the collection will indicate that providing the information is voluntary.

(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.

(U) the Privacy Act Statement will inform the applicant of the use. Since providing the information is voluntary, there is assumed consent when an applicant submits his/her application for consideration.

(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.

(U) When applicants apply to the scholarship program, they are asked to provide PII data. Applicants are shown a Privacy Act statement describing the reason for collecting the information, the fact that providing the information is voluntary, and the potential consequences for not providing the information.

(U) Authority for collecting information requested on the DoD Information Assurance Scholarship Program Application is contained in 5 U.S.C. Sections 4101-4121, 10 U.S.C. §2200, Executive Order 13111, Executive Order 11348, as amended, and DoD Directive 8500.2. DoD's Blanket Routine Uses (found at Appendix C of 32 CFR Part 310) and the specific uses found in GNSA27 apply to this information. The requested information will be used to determine eligibility for the Information Assurance Scholarship Program. Disclosure of the requested information is voluntary. However, failure to provide the requested information will prevent the processing of your application and the determination of your eligibility for the Information Assurance Scholarship Program.

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 can restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply in the table below.

☒ Name	☒ Other Names Used	☐ Social Security Number (SSN)
☐ Truncated SSN	☐ Driver's License	☐ Other ID Number
☒ Citizenship	☐ Legal Status	☐ Gender
☐ Race/Ethnicity	☐ Birth Date	☐ Place of Birth
☒ Personal Cell Telephone Number	☒ Home Telephone Number	☒ Personal E-mail Address
☒ Mailing/Home Address	☐ Religious Preference	☒ Security Clearance
☐ Mother's Maiden Name	☐ Mother's Middle Name	☐ Spouse Information
☐ Marital Status	☐ Biometrics	☐ Child Information
☐ Financial Information	☐ Medical Information	☐ Disability Information
☐ Law Enforcement Information	☒ Employment Information	☒ Military Records
☐ Emergency Contact	☒ Education Information	☒ Other

If "Other," specify or explain any PII grouping selected.

(U) Social Security Numbers may be submitted by a DoD student applicant due to the application requirements. The DoD IASP Program Office does not need SSNs to process the scholarship application. In many cases applicants are told to strike-out/black-out their SSN on any and all forms.

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

(U) Individual

(3) How will the information be collected? Indicate all that apply.

☒ Paper Format
☐ Face-to-Face Contact
☐ Telephone Interview
☒ Fax
☒ E-mail
☐ Web Site
☐ Information Sharing from System to System
☐ Other (Describe)

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

(U) verification - The DoD IASP Program Office will use the information provided by the applicant with that provided by the university or component to verify the individual is who they say they are.
identification - n/a
authentication - n/a
data matching - The DoD IASP Program Office uses the information provided by the applicant to validate the data provided is accurate and correct.

(5) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

(U) Administrative use

b. Does this DoD information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes** ☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in the DoD information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☐ **Other** (Describe)

d. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards ☐ Cipher Locks ☒ Identification Badges

☐ Combination Locks ☐ Key Cards ☐ Closed Circuit Television

☐ Safes ☐ Other (Describe)

(2) **Technical Controls.** Indicate all that apply.

- [X] User Identification
- [X] Password
- [ ] Intrusion Detection System (IDS)
- [ ] Encryption
- [ ] External Certificate Authority (CA) Certificate
- [ ] Common Access Card (CAC)
- [X] Other (Describe)

(U) Data files are separated from normal office business and only accessible by DoD IASP Team members.

- [ ] Biometrics
- [ ] Firewall
- [ ] Virtual Private Network (VPN)
- [ ] DoD Public Key Infrastructure Certificates

(3) **Administrative Controls.** Indicate all that apply.

- [ ] Periodic Security Audits
- [ ] Regular Monitoring of Users' Security Practices
- [X] Methods to Ensure Only Authorized Personnel Access to PII
- [ ] Encryption of Backups Containing Sensitive Data
- [ ] Backups Secured Off-site
- [ ] Other (Describe)

e. Does this DoD information system require certification and accreditation under the NSA/ CSS Certification and Accreditation Process?

- [X] **Yes.** Indicate the certification and accreditation status:
  - [X] Authorization to Operate (ATO) Date Granted: 02/29/2012
  - [ ] Interim Authorization to Operate (IATO) Date Granted:

☐ Denial of Authorization to Operate (DATO) Date Granted:

☐ Interim Authorization to Test (IATT) Date Granted:

☐ **No**, this DoD Information system does not require certification and accreditation.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

(U//FOUO) For information handling at each stage:
a. Collection: Hard-copy applications are stored in locked flippers. Electronic-copy applications received via CDs are virus scanned and stored in a separate file only accessible by DoD IASP team members.
b. Use: Files are placed in shared hard copy files and electronic directories and retrieved by DoD IASP team members only.
c. Retention: Maintain as open files until the grant is completed and/or payment obligation as annotated in the student agreement is completed. Transfer closed files to the NSA/CSS Records Center. Destroy 5 years after transfer. (N1-457-07-001)
d. Disclosure: The DoD IASP Program Office provides the information to DoD components who participate in the recruiting and nominating of students. The Human Resources and Recruitment offices at DoD components may also have access to the data. Request to view the data must be approved by the DoD IASP Program Office.
e. Destruction: Records are destroyed by pulping, burning, shredding, or erasure or destruction of electronic media.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks?

(U//FOUO) Access to shared directories is accessed by valid login/password by only DoD IASP team members. Access to the directory is deleted and passwords are changed should an individual leave the team. To mitigate the risk from the privilege user, the DoD IASP team is required to complete annual mandatory PII Privacy training. To mitigate the risk of malicious code the CDs/ electronic files are virus scanned.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

N/A

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program or Project Manager (could be System Developer, System Owner, Data Owner or Designee)

Signature: Shaffer Alice Elizabeth aeshaff Digitally signed by Shaffer Alice Elizabeth aeshaff DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=0002, cn=Shaffer Alice Elizabeth aeshaff Date: 2012.12.11 15:57:28 -05'00'

Name: Alice E. Shaffer

Title: DoD IASP Recruitment and Grant Program Manager (System Developer/Owner)

Organization: I084

Work Telephone Number: 968-8811s / 410-854-6206b

DSN:

Email Address: aeshaff@nsa.ic.gov

Date of Review: 12/11/2012

NSA/CSS Government Supervisor

Signature: Tancock Carolyn Kramer cktanco Digitally signed by Tancock Carolyn Kramer cktanco DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=0002, cn=Tancock Carolyn Kramer cktanco Date: 2012.12.12 11:08:41 -05'00'

Name: Carolyn K. Tancock

Title: Chief, National Information Assurance Education and Training Program

Organization: I084

Work Telephone Number: 968-8811s / 410-854-6206b

DSN:

Email Address: cktanco@nsa.ic.gov

Date of Review:

NSA/CSS Designated Approving Authority Representative

Signature: Goranson John Richard jrgoran

Digitally signed by Goranson John Richard jrgoran
DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=D002, cn=Goranson John Richard jrgoran
Date: 2012.12.18 10:49:05 -05'00'

Name: Rich Goranson

Title: Designated Authorizing Official

Organization: TS14

Work Telephone Number: 303-1225

DSN:

Email Address: jrgoran@nsa.ic.gov

Date of Review: 12/18/2012

NSA/CSS Designated Approving Authority

Signature: Schaffer Jean Holdridge jhschaf

Digitally signed by Schaffer Jean Holdridge jhschaf
DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=D002, cn=Schaffer Jean Holdridge jhschaf
Date: 2012.12.19 14:54:36 -05'00'

Name: Jean Schaffer

Title: Authorizing Official

Organization: TS

Work Telephone Number: 303-1500

DSN:

Email Address: jhschaf@nsa.ic.gov

Date of Review: 12/19/2012

NSA/CSS Privacy Advocate

Signature: Grein Kristina Marie kmgrein Digitally signed by Grein Kristina Marie kmgrein DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=D002, cn=Grein Kristina Marie kmgrein Date: 2012.12.12 12:49:39 -05'00'

Name: Kristina Grein

Title: NSA/CSS Privacy Advocate

Organization: DJ4

Work Telephone Number: 240-373-9745

DSN:

Email Address: kmgrein@nsa.gov

Date of Review: 12/12/2012

NSA/CSS CIO

Signature: Miller Kelly Alan kamill4 Digitally signed by Miller Kelly Alan kamill4 DN: c=US, o=U.S. Government, ou=DoD, ou=NSA, ou=D002, cn=Miller Kelly Alan kamill4 Date: 2013.01.07 08:20:35 -05'00'

Name: Kelly Miller

Title: D/CIO

Organization: T

Work Telephone Number:

DSN:

Email Address:

Date of Review:

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.

APPENDIX

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

DoD Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection of Information. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, DoD dependents are considered members of the general public.

Personally Identifiable Information. Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a DoD Web site (e.g., collected as part of an email feedback/comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.