GNSA 27

System name:

Information Assurance Scholarship Program

System location:

National Security Agency/Central Security Service, Ft. George G. Meade, MD 20755-6000

Categories of individuals covered by the system:

Individuals and institutions who apply for recruitment scholarships, retention scholarships or grants under the DoD Information Assurance Scholarship Program (IASP).

Categories of records in the system:

Information is to be collected on the following aspects of the IASP: the recruitment program; the retention program; the capacity-building program; and the assessment program.

For individuals participating in the recruitment program, the information collected for the selection process includes: title, full name, current address, permanent address, phone number, cell phone number, e-mail addresses, two letters of reference, self-certification of US citizenship, certification that official transcripts are provided, GPA, SAT and GRE test scores, self-certification of enrollment status at a CAE, anticipated date of graduation, resume (to include non-work activities such as community outreach, volunteerism, athletics, etc.), a list of awards and honors, veteran status, OF 612 (Job Vacancy Application for the position the individual will fill on completion of the program), and desired DoD Agency (first, second, and third choices). This information is provided to the IASP program office through the school the prospective scholarship recipients is attending.

For individuals participating in the retention program, the information collected for the selection process includes: full name; office address; office phone number; office fax number; office email address; list of previous post-secondary schools attended, including School Name, Degree/Certificate (if earned), and GPA; official transcripts from all schools attended; proposed university(ies); proposed degree; proposed start date for the program; proposed student status (full-time/part-time); anticipated date of graduation; *Continued Service Agreement(SF-182); resume; personal goals statement; two letters of

recommendation (supervisor and next level); GRE or GMAT scores; and documentation of the applicant's security clearance. Additionally, the following is required of the applicant's supervisor: name, official title, office email address, and office phone number. The following is required of the Component's Office of Primary Responsibility: name, title, office address, office email address, and office phone number.

*Note: *Components request a Continued Service Agreement (SF-182) as part of the retention scholarship award process. The form contains Personally Identifiable Information, including the applicant's social security number. Since the requirement is generated by the Component, they are responsible for maintaining the SF-182 as part of the scholarship recipient's personnel record. The IASP Program Office receives a copy of the completed form during the retention nomination process, but does not request the social security number as a part of the program requirement.*

Institutions participating in the capacity-building program must provide a detailed description of the proposed project, including a cost breakout of each aspect of the proposal.

IASP scholars and participating institutions are required to complete periodic program assessment documents, forwarded to them from the DoD. In general, the information requested relates to the respondent's overall assessment of the program, and suggestions for improvements.

Authority for maintenance of the system:

Sections 2200 et seq. and 7045 of title 10, United States Code; Deputy Secretary of Defense Memorandum, "Delegation of Authority and Assignment of Responsibility under Section 922 of the Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001," June 26, 2001

Purpose(s):

The DoD Information Assurance Scholarship Program (IASP) is designed to increase the number of new entrants to DoD who possess key Information Assurance (IA) and Information Technology (IT) 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. Applicants eligible for this program must attend, or be accepted to attend one of the institutions designated by the National Security Agency (NSA)and the Department of Homeland Security as a National Center of Academic Excellence in

Information Assurance Education (CAE/IAE) or Research (CAE-R). These institutions are collectively referred to as CAEs.

The program consists of two tracks: recruitment and retention. Both tracks require a service commitment to DoD. The IASP recruitment program is for college students who, on completion of the program come to work for DoD in critical IA/IT jobs. The retention program is for current DoD employees (civilian and military) whom take advanced college courses in IA/IT disciplines for professional development. Pending availability of funds, the IASP may also award capacity building grants to CAEs for such purposes as developing IA curricula, faculty, and laboratories and for modest research linked to student and/or faculty development in IA. There is an assessment process for CAEs, which examines how grant funds were spent as well as an assessment process requiring status reports from students in the program, their supervisors, and university faculty representatives (Principal Investigators) for the purpose of the periodic program reviews.

The recruitment, retention, and grant program all require a competitive application process. In order to apply for any aspects of the program, paperwork is required so that the DoD may judge the merits of a given application and determine how best to allocated IASP funds. This will enable the Information Assurance Scholarship Program to select qualified applicants and institutions to be awarded scholarships and capacity building grants.

Additionally, the IASP may periodically conduct performance surveys with IASP scholars and CAEs in an effort to continually improve the program.

The recruitment, retention, capacity building, assessment and survey aspects of the IASP apply to non-DoD employees, DoD active duty military members and permanent DoD civilian employees who choose to become involved in the program and thus become subject to said information collection requirements.

The Director of NSA, under the authority, direction, and control of the Under Secretary of Defense for Intelligence, serves as the DoD IASP Executive Administrator to:

(1) Implement the DoD IASP and publish in writing all of the criteria, procedures, and standards required for program implementation and,

(2) Subject to availability of funds, make grants on behalf of the Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer to CAEs to support the establishment, improvement, and administration of IA education programs.

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, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To authorized federal hiring officials to facilitate the recruiting of DoD IASP award recipients into federal service for the purpose of fulfilling the DoD IASP mission.

Disclosure to consumer reporting agencies:

Disclosures pursuant to 5 U.S.C. 552a(b)(12) may be made from this system to `consumer reporting agencies' 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)). 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.

The disclosure is limited to information necessary to establish the identity of the individual, including name, address, and taxpayer identification number (Social Security Number); the amount, status, and history of the claim; and the agency or program under which the claim arose for the sole purpose of allowing the consumer reporting agency to prepare a commercial credit report.

The DoD "Blanket Routine Uses" set forth at the beginning of the NSA/CSS' compilation of systems of records notices apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records in file folders and electronic storage media.

Retrievability:

Retrieved by the individual’s name, institution’s name and/or year of application.

Safeguards:

Paper and electronic media containing information is restricted to those who require the data in the performance of their official duties. Access to information is further restricted by the use of passwords that are changed periodically. Physical entry is restricted by the use of locks, guards, and administrative procedures. Contract officers are required to incorporate all appropriate Privacy Act clauses.

Buildings are secured by a series of guarded pedestrian gates and checkpoints. Access to facilities is limited to security-cleared personnel and escorted visitors only. Within the facilities themselves, access to paper and computer printouts are controlled by limited-access facilities and lockable containers. Access to electronic means is limited and controlled by computer password protection.

Retention and disposal:

Records are destroyed when 5 years old or when superseded or obsolete whichever is sooner.

Records are destroyed by pulping, burning, shredding, or erasure or destruction of electronic media.

System manager(s) and address:
DoD IASP Executive Administrator, National Security Agency/Central Security Service,9800 Savage Road, Fort George G. Meade, Maryland 207855-6000.

Notification procedures:

Individuals seeking to determine whether records about themselves is contained in this record system should address written inquiries to the National Security Agency/Central Security Service, Freedom of Information Act/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, Maryland 207855-6248.

Requests should contain the individuals name, address, award year and type, and the institution attended.

Record Access procedures:

Individuals seeking access to information about themselves contained in this system should address written inquiries to the National Security Agency/Central Security Service, Freedom of Information Act/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, Maryland 207855-6248.

Requests should include individuals name, address, award year and type, and the institution(s) attended. All requests must be signed.

Contesting record procedures:

The NSA/CSS rules for contesting contents and appealing initial agency determinations may be obtained by written request addressed to the National Security Agency/Central Security Service, Freedom of Information Act (FOIA)/Privacy Act Office, 9800 Savage Road, Suite 6248, Ft. George G. Meade, MD 20755-6248.

Record source categories:

Individuals, via the IASP recruitment or retention application process; CAEs/Institutions via the grants application process.

Exemptions claimed for the system:

None.