Department of Defense
Information Assurance Scholarship Program

Sponsored by the

DoD Chief Information Officer

SOLICITATION FOR PROPOSALS

From
Universities Designated by the
National Security Agency (NSA) and the Department of Homeland Security (DHS)
as
National Centers of Academic Excellence in Cyber Defense Education
and
National Centers of Academic Excellence – Research,
(herein after referred to as CAEs)
and
Universities Designated by the
National Security Agency
as
National Centers of Academic Excellence – Cyber Operations

Issued by the National Security Agency on behalf of the Department of Defense

Proposal Submission: 31 May 2017

SUBJECT TO AVAILABILITY OF FUNDS

April 2017

CONTENTS

DEPARTMENT OF DEFENSE
INFORMATION ASSURANCE SCHOLARSHIP PROGRAM

SOLICITATION

I. INTRODUCTION

The Department of Defense (DoD) Information Assurance Scholarship Program (IASP) was established, in accordance with provisions of Chapter 112, "Information Security Scholarship Program," of title 10, United States Code, added by Public Law 106-398, The National Defense Authorization Act for fiscal year 2001. The purpose of the program is to increase the number of qualified students entering the fields of information assurance, information technology, and cybersecurity to meet the DoD's increasing dependence on cybersecurity for war fighting and the security of its information infrastructure.

Regionally and nationally accredited U.S. institutions of higher education, designated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as National Centers of Academic Excellence in Cyber Defense Education or National Centers of Academic Excellence in Cyber Defense Research and designed by the National Security Agency (NSA) as National Centers of Academic Excellence – Cyber Operations (hereinafter referred to as CAEs) are invited to submit proposals for developing and managing a full-time, institution-based, grant-funded scholarship program in the disciplines underpinning cybersecurity for Academic Year 2017-2018. CAEs may propose collaboration with other accredited institutions, and are encouraged to include accredited post-secondary minority institutions.

Consistent with 10 U.S.C. 2200b, CAE proposals to this solicitation may also request modest collateral support for purposes of institutional capacity building to include faculty development, laboratory improvements, and/or curriculum development, in cybersecurity related to providing a strong foundation for a Information Assurance Scholarship Program. [Special note: Requirements for proposing modest capacity building support are detailed in ANNEX II.

To continue the development of a strong foundation for the scholarship program during the Academic Year 2017-2018, competition will be limited to full-time students entering their third or fourth years of undergraduate education; students in their first or second year of a master's degree program; students pursuing doctoral degrees.

II. TERMINOLOGY

A. Cybersecurity: For purposes of this program, the term Cybersecurity encompasses the scientific, technical, and management disciplines required to ensure computer and network security including the following functions:

- System/network administration and operations
- Systems security engineering
- Information assurance systems and product acquisition
- Cryptography
- Threat and vulnerability assessment, to include risk management
- Web security
- Operations of computer emergency response teams
- Information assurance training, education and management

- Computer forensics
- Defensive information operations
- Critical information infrastructure assurance

Relevant academic disciplines, with concentrations in cybersecurity, would include, but are not limited to:

i. Biometrics
ii. Business:
   1. Management
   2. Administration
   3. Process Analysis

iii. Computer:
   1. Crime Investigations
   2. Engineering
   3. Forensics
   4. Information Science
   5. Information Systems
   6. Programming
   7. Science
   8. Systems Analysis

iv. Critical Information Infrastructure Assurance
v. Cyber:
   1. Operations
   2. Security
   3. Policy

vi. Cryptography
vii. Database Administration
viii. Data Management
ix. Digital and Multimedia Forensics
x. Electrical Engineering
xi. Electronics Engineering
i. Information Assurance:
   1. Systems and Product Acquisition
   2. Training, Education and Management

xii. Information Security (Assurance)
xiii. Information Systems
xiv. Information Technology:
   1. Acquisition
   2. Program/Project Management

xv. Mathematics
xvi. Network Administration and Operations
xvii. Network Management
xviii. Operation of Computer Emergency Response Teams
xix. Software Engineering
xx. Systems Security Engineering
ii. Threat and Vulnerability Assessment, to include Risk Management
iii. Web Security
iv. And other similar disciplines as approved by the DoD Chief Information Office (DoD CIO).

B. The opportunity exists for part-time Government (DoD) employment while receiving scholarship (see Student Application), through the Agency intern and hiring options, to include the authority to employ individuals completing Department of Defense Scholarship or Fellowship programs, and/or the related "r" waiver authority.

III. OVERVIEW OF PROGRAM SCOPE

The key elements of the DoD IASP, and the CAE's role in the process, are addressed in the subsections that follow. University grantees will be required, as a condition of grant award, to establish and manage the program*, including disbursement of scholarship funds to students. Grant awards are made to the universities, not directly to the students*.

A. Academic Year 2017-2018 The DoD estimates awarding scholarships (via grant awards) for a period of one year (beginning with the fall 2017 semester) to designated CAEs, operating independently or in collaboration with other accredited institutions, including accredited post-secondary minority institutions. The purpose is to lay a sound foundation for the development of a robust information assurance program for undergraduate and graduate students enrolled in the CAE or its collaborating institutions' degree and graduate certificate information assurance programs. To this end, institutions receiving grants will be required to conduct a self-evaluation to identify improvements in program design and management for implementation in future years. In addition to proposing establishment of an Cyber scholarship program within the university, CAEs may also request funds for capacity building activities. Grant awards are contingent upon availability of funds.

B. Capacity Building: **This particular area is subject to the availability of funds**. In accordance with 10 U.S.C. 2200b, CAEs may request modest support for building the institution's capacity for research and education in cybersecurity in addition to the scholarship proposals. The DoD has determined focus areas for this opportunity. Proposals submitted should reflect student engagement: opportunities for the CAE students to participate and gain additional understanding of cybersecurity as it relates to the extended community and DoD.

The two focus areas are DoD Partnerships and Outreach to Technical Colleges, Community Colleges, and/or Minority Institutions. Activties that may support these topics may include but are not lmited to: **1) Faculty development**, **2) Facility/Lab/Technology development and/or, 3) Curriculum development**.

Details for all activities will be described in ANNEX II. CAE requests for capacity building support should be part of the overall insitutional submission, but identified in it's how section of the submission. Narravtives for the scholarship and capacity buidling portions should be severalable from each other

D. Proposal Formats: At a minimum and to be eligible to sumit a capacity building propsal, the sumbission must respond to the establishment of a Information Assurance Scholarship Program (Basic / recruitment).

E. The DoD IASP Application Due Dates: CAEs electing to submit a proposal to establish a scholarship program must ensure that they establish a due date for student scholarship applications that will allow them sufficient time to evaluate the student applicants and prepare their recommendations of student candidates for postmarking or emailing on/before **Wednesday 31 May 2017**, These dates are critical in order to ensure grant awards as close to August 1, 2017 as possible. See Section XII, "Deadline for Submission", for dates and Attachment A "Proposal Preparation Instructions and Certifications" for details on submission requirements.

F. The DoD Role: While CAEs are required to provide the DoD an assessment of each applicant, the actual selection of student scholars will be made by DoD evaluators. Students selected as Information Assurance Scholars will receive the full cost of tuition, books (from the institution/ degree specific required book list, not books which are optional for the class), required fees (including health care), and a stipend to cover room and board. The stipend levels are $22,500 for undergraduate students and $30,000 for graduate (Master's/PhD) students. Awards will be made via a grant to the CAE. Selecting agencies will also provide sponsors who will maintain contact with the student during the scholarship period, and who will facilitate the student's entry into internships, if applicable, and eventually DoD employment. The DoD IASP Program Office will contact CAEs submitting successful proposals to develop agreements governing the character, scheduling, and periodic assessment of student internships.

G. Future Opportunities for Returning Students: Contingent on adequate funding appropriations, it is anticipated that current CAE grantees and successful scholarship recipients will receive follow-on support to complete their degree program. Returning students will be required to re-apply each year by submitting the entire student application, one copy of their official transcripts, reflecting maintenance of the required grade point average and an endorsement/ recommendation letter from the Principal Investigator.

IV. STUDENT OBLIGATIONS

Students selected to participate in the DoD IASP will be required to sign a written agreement obligating them to work for the DoD, as a civilian employee for one calendar year for each year of scholarship assistance. However, should a student apply for only one semester (or six months) of scholarship, the student must still agree to work for the DoD for one year. This agreement is provided to the selecting agency for their records to ensure compliance with the service commitment. Students will also be required to serve in internship positions, if timing permits, with the DoD organizations during the time they are receiving scholarship support until they complete the course of study provided for by the scholarship. These internships will be arranged by the DoD to occur during the summer or other breaks between school terms, as appropriate to the individual's circumstances and the institution's calendar. The internship does not count toward satisfying the period of obligated service incurred by accepting the scholarship. Students will be required to formally accept or decline the scholarship within 15 days of notification. Non-acceptance by this date will mean the scholarship will be offered to the next available student.

Students will be required to complete a security investigation questionnaire to initiate the process for a background investigation in preparation for their internships, if applicable, and as a condition of future employment with the DoD. Drug tests or other suitability processing will occur as appropriate. Students will also be required to sign an agreement stating that they will accept assignments requiring travel or change of duty stations as interns or employees. Individuals who voluntarily terminate employment during intern appointments or before the end of the period of obligated service required by the terms of Chapter 112, title 10, United States Code, will be required to refund the United States, in whole or in part, the cost of the educational assistance provided to them. Web pages have been provided in the Application Background and Application Package for review about security clearances to assist both the PIs and the students in understanding these requirements before they apply.

[1] If a student is applying for only one half of a school year (or graduates 1 semester early), that student shall only receive half the stipend amount. The stipend is based upon an annual full-time attendance at the CAE. Students planning to graduate in December 2017, must be clearly identified (**for placement purposes**).

An opportunity also exists for scholarship payback through military service. Individuals choosing to enlist or accept a commission to serve on active duty in one of the Military Services shall incur a service obligation of a minimum of 4 years on active duty in that Service upon graduation. The Military Services may establish a service obligation longer than 4 years, depending on the occupational specialty and type of enlistment or commissioning program selected.

Undergraduate scholarship recipients will be required to maintain a 3.2 out of 4.0 grade point average or the equivalent; graduate students will be required to maintain an overall 3.5 out of a 4.0 grade point average, or equivalent. Failure to maintain satisfactory academic progress will constitute grounds for termination of financial assistance and termination of internship and/or employment appointment. Additionally, students who fail to complete the degree program satisfactorily or to fulfill the service commitment upon graduation shall be required to reimburse the United States, in whole or in part, the cost of the financial (scholarship) assistance provided to them. CAEs will be responsible for monitoring student progress and will notify the DoD IASP Program Manager should any student scholar fail to attain minimum academic standards required for continuing scholarship support.

Except for small achievement awards, not to exceed $5,000 in any academic year, a student may not accept simultaneous remuneration from another scholarship or fellowship.

Graduate programs may include a reasonable amount of teaching or similar activities that are, in the CAE's opinion, contributory to the student's academic progress; however, the development of students, not service to the CAE, will govern the assignment of these activities.

V. CONDITIONS OF THE GRANT COMPETITION

In order to be competitive in this grant solicitation, CAEs must be willing to advertise and manage a competition for scholarship applicants; conduct an evaluation of applicants' qualifications and abilities; and submit ***all*** the applications received to the DoD, along with the CAE's assessment and recommendation of each proposed scholar's capabilities and potential. CAEs are reminded to establish a date for student application submissions that will allow sufficient time for this process. The specific requirements for advertising the scholarship among the candidate student populations, collecting and assessing student applications, and reporting on the process are addressed below in paragraph VII below. Proposal evaluation criteria will review how well CAEs conduct the recruitment and assessment process.

VI. CAE ROLE IN RECRUITING AND ASSESSING SCHOLARSHIP CANDIDATES

If a CAE decides to participate in this portion of the grant competition, the following requirements apply:

A. Announcing and Promoting the Program: The CAE wishing to submit a proposal will be expected to take the following actions, at a minimum, to promote student interest in the DoD Cy scholarship opportunity:

1. Determine and communicate to the relevant student populations any CAE unique conditions, instructions, and/or materials (including due dates) that are associated with the acceptance of applications for the DoD IASP opportunity.

2. Publish and ensure that all appropriate DoD IASP application materials are made available to all relevant student populations. This includes providing equal access to hard copy and soft copy application documents/materials, any CAE and the DoD unique instructions, notices of deadlines; and any additional required information about the DoD IASP.

B. Managing the Application Review and Candidate Assessment Process: CAEs electing to propose establishment of a scholarship program are required to verify each applicant's eligibility for scholarship and academic sufficiency, to evaluate each eligible candidate's knowledge and ability in certain competency areas important to successful information assurance work, and to provide a relative endorsement level for each eligible candidate. CAEs may determine the procedures to be followed in conducting the evaluation, including records verification, individual interviews, faculty review panels, as long as all applicants are afforded full and equal opportunity for consideration in appropriate review phases.

1. Eligibility for Scholarship and DoD Appointment. CAEs shall verify documentation of the eligibility of each applicant for scholarship and appointment and shall exclude from further evaluation any applicant unable to meet the minimum administrative requirements which are noted in Attachment C, DoD Information Assurance Scholarship Application Background and Requirements. ***Current DoD/Federal Employees, Active Duty Military/Reserves/Guard, or students with an exisiting service obligation are not eligible to apply.***

2. CAE Endorsement. **Please use Attachment E, Cost and Student Endorsement and Rank Form, for the following:** CAEs shall provide an endorsement of each applicant meeting administrative and academic sufficiency requirements that is based on the overall evaluation of all applicant materials, including the competency evaluations described above. CAEs shall indicate only one of the following **three levels** of endorsement for each applicant:

    a. **Not Recommended**
    b. **Recommended**
    c. **Highly Recommended**

C. Submitting Student Scholarship Applications and CAE Review and Endorsement: CAEs that propose to support the scholarship program are required to receive and submit all applications in response to the announcement and to evaluate the applicants as described in detail above. See instructions on requirements and submissions in the Attachment A, Proposal Preparation Instructions. All applications, including those not recommend must be included in the submission.

VII. TECHNICAL PROPOSALS

See instructions on requirements and submissions in Attachment A, Proposal Preparation Instructions.

VIII. COST PROPOSALS

The cost proposal information can be found in Attachment A, Proposal Preparation Instructions.

IX. GRANT PROPOSAL EVALUATION CRITERIA AND SELECTION PROCESS

Proposals will be evaluated by a panel of Department of Defense specialists in Cybersecurity drawn from the Military Departments, the Office of the DoD Chief Information Officer, the National Security Agency, and other DoD Components. Proposals will be evaluated against the following criteria:

A. The merits of the institution's proposed approach to designing and developing a robust Information Assurance Scholarship Program and the likelihood of its producing the highest quality scholars for the DoD employment.

B. The quality of the institution's process for promoting and advertising the IASP opportunity and evaluating students for scholarship and the DoD appointment, and the effectiveness of this process in producing well-qualified candidates for the DoD selection.

C. The proposed program's congruence with statutory intent, the requirements of the DoD, and its relevance and potential contribution to the DoD mission needs.

D. The qualifications of key faculty, staff and advisors and their proposed role in the scholarship program.

E. The adequacy of the institution's existing resources to accomplish the program objectives.

F. The realism and reasonableness of the cost proposal.

X. AWARDS

Scholarship notifications for students will be announced to the CAEs in the June 2017 time frame. The grants for Scholarships (Basic) and ANNEX II will be awarded in the July/August 2017 timeframe. Awards will be made for one year only. The DoD may award a lower level of funding than that proposed.

The DoD recognizes the considerable CAE investment required to conduct the student recruitment and assessment process, and to develop and submit a competitive proposal in this competition. Depending on the availability of funds, the DoD may elect to award capacity grants to CAEs that have submitted outstanding proposals, and have managed the recruitment and assessment process in an exceptional manner, but whose student candidates the DoD may not select in the competition for scholarship and the DoD appointments. Because expectations are that the program will grow in future years, these program awards should enable CAEs to complete planning for implementing a comprehensive scholarship program and be prepared to manage succeeding rounds of student recruitment.

However, as in the case of the capacity grants described above, the institution's technical proposal must demonstrate exceptional merit and potential for full implementation in succeeding phases of student recruitment and selection.

XI. OTHER ITEMS

Individuals supported by a grant awarded as a result of this solicitation must be U.S. Citizens, or permanent residents admitted to the U.S. for permanent residence prior to award. To be eligible for an award, an organization must submit a certificate of Assurance or Compliance with Title VI of the Civil Rights Act of 1964 and be constantly in compliance with the Act.

As indicated in Executive Order 12549, "...Executive departments and agencies shall participate in a government wide system for non-procurement debarment and suspension. A person who is debarred or suspended shall be excluded from Federal financial and non-financial assistance benefits under Federal programs and activities. Debarment or suspension of a participant in a program by one agency shall have a government wide effect."

XII. SYSTEM OF AWARD MANAGEMENT (SAM)

SAM is the primary Government repository for prospective federal awardee information and the centralized Government system for certain contracting, grants, and other assistance related processes. All contractors must be registered in the SAM to receive solicitations, awards, or payments. To register in the SAM, you may use any one of the following methods: (1) telephone: 1-866-606-8220; (2) input directly to the SAM through the internet at: https://www.acquisition.gov. Processing time for registration of an application submitting an application may take up to five (5) business days. Should you need additional information, visit their home page at: http://www.sam.gov.

XIII. SYSTEM OF AWARD MANAGEMENT (SAM)

"Acquisition Resource Center (ARC) Business Registry means the primary Maryland Procurement Office (MPO) repository for contractor information required for the conduct of business with MPO. "Registered in the ARC Business Registry" means that all mandatory information is included in the ARC Business Registry. By submission of an offer, the offeror acknowledges the requirement that a prospective awardee must be registered in the ARC Business Registry prior to award, during performance, and through payment of any contract resulting from this solicitation. Lack of registration in the ARC Business Registry shall make an offeror ineligible for award. MPO established a goal of registering all contractors in the ARC Business Registry to provide a market research tool and to facilitate communication between the MPO and the contractor community. Offerors that are not already registered in the ARC should apply for registration immediately upon receipt of this solution. The Contractor is responsible for the accuracy and completeness of the data within the ARC, and of any liability resulting from the Government's reliance on inaccurate or incomplete data. The Contractor agrees to periodically update information when previously provided information changes. To remain registered in the ARC Business Registry after the initial registration, the Contractor is required to confirm annually on or before the anniversary of the initial registration that the information is accurate and complete. Offerors that are not already registered in the ARC Business Registry shall register via the internet at: http://www.nsaarc.net/

XIV. DEADLINE FOR SUBMISSION

See the proposal preparation instructions for details on the submission of proposals. Institutionally approved, signed, completed proposals which include all items listed above and all student applications must be **postmarked or emailed on/before Wednesday, 31 May 2017**.

XV. LATE SUBMISSIONS

The CAE is responsible for submitting the proposal and student materials to the DoD IASP Program Office at the National Security Agency by the date and time specified.

Proposals or student materials that are postmarked after the deadline of 31 MAY 2017, are "late" and will not be considered for an award or scholarship.

XVI. INCOMPLETE PROPOSALS

Proposals or student materials submitted in the wrong format, using wrong forms, or missing items will be deemed incomplete and will not be considered for an award of scholarship program selection.

XVII. CONTACT INFORMATION

The central DoD IASP Points of Contact for information regarding this solicitation are:

DoD IASP
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755-6804

e-mail: askiasp@nsa.gov
410-854-6206

ANNEX II
Institutional Capacity Building

CAEs *may, but are not required to*, address this section of the solicitation with a separate ANNEX II to their proposals titled "Proposal for Capacity Building." Funds for ANNEX II may be awarded only if the institution submits a qualified basic proposal. Specific projects should be identified and addressed separately. This submission will be evaluated separately from the CAE's basic proposal in response to the broader solicitation. **While scholarships will be funded prior to any capacity building, approximately $1,000,000 will be set aside for capacity building.**

CAEs may sumbit one proposal which provides a response to one or both of the two focus areas identified below. The total proposal submission per CAE should not exceed $125,000. As a result, all proposal(s) submitted should clearly articulate the expected benefits and impact to the Department of Defense (DoD) and/or the broader community.

I. OVERVIEW

In accordance with 10 U.S.C. 2200b, CAEs may request modest support for building the institution's capacity for research and education in information assurance. The DoD has determined focus areas for this opportunity. Proposals submitted should reflect student engagement: opportunities for the CAE students to participate and gain additional understanding of Cybersecurity as it relates to the extended community and DoD.

1. **DoD Partnerships:** To increase the knowledge and skills of students & DoD partners in the areas of IA, IT, and Cybersecurity. The goals should include providing students & DoD partners with hands-on, real-world opportunities, while improving existing DoD programs and projects.
    a. **Faculty Development:** Provide experiential learning opportunities for cyber faculty and students (i.e., hands-on training in the appropriate academic topics identified in Section II. Terminology and/or including ethical hacking, SCADA, penetration testing, digital forensics and social engineering); develop scenario-based exercises and simulation tools.

    b. **Facility / Lab / Technology Development:** Provide lab exercises and/or equipment that may be accessible by other department and institutions & DoD partners (i.e., to test software and/or provide hands-on instruction).

    c. **Curriculum Development**: Develop curriculum and toolsets for critical cybersecurity topics such as cybersecurity, secure programming, SCADA, and ethical hacking, that may be downloaded or offered as shared module; develop a security awareness module for cross-departmental and community use.

2. **Outreach to Technical Colleges, Community Colleges, and/or Minority Institutions**[1]: To increase the pipeline of students in the areas of Cybersecurity. The goal should be to build stronger educatio programs in these areas to advance the state of the nation and to grow and expand the pool of qualified candidates for futre employement. Proposals should include short-term objectives and expected long-term benefits of the collaborative partnerships with technical colleges, community colleges, or minority institutions.

[1] *The U. S. Department of Education reference for minority institutions is located at: http://www2.ed.gov/about/offices/list/ocr/edlite-minorityinst-list-tab.html and the United States code 20 U.S.C. 1067k refers to the term "minority institution" as an institution of higher education whose enrollment of a single minority or a combination of minorities include: American Indian, Alaskan Native, Black (not of Hispanic origin), Hispanic (including persons of Mexican, Puerto Rican, Cuban, and Central or South American origin), or Pacific Islander.*

a. **Faculty Development**: Provide experiential learning opportunities for cyber faculty and students (i.e., hands-on training in the appropriate academic topics identified in Section II. Terminology and/or including ethical hacking, SCADA, penetration testing, digital forensics and social engineering); develop scenario-based exercises and simulation tools

b. **Facility/Lab/Technology Development**: Provide lab exercises and/or equipment that may be accessible by other department and institutions & DoD partners (i.e., to test software and/or provide hands-on instruction).

c. **Curriculum Development**: Develop curriculum and toolsets for critical cybersecurity topics such as cybersecurity, secure programming, SCADA, and ethical hacking, that may be downloaded or offered as shared module; develop a security awareness module for cross-departmental and community use.

Examples of activities that may support proposals in these areas include:

a. Laboratory equipment[2] purchase and/or installation and lab exercises to be provided at non-CAE institutions. These activities would afford the students from the different academic populations to gain: hands-on experience; a better understanding of the Cybersecurity career fields and increased awareness of the potential security threats, vulnerabilities, and knowledge on improving the security posture for themselves and others around them.
b. Faculty and student projects in information technology/security in order to develop a strong foundation for an Information Assurance Program.
c. Partnerships with DoD organizations and installations in the area of exercises and labs that improve their ability to train and educate their IA/IT and Cybersecurity workforce;
d. Partnerships with the DoD Wounded Warriors and returning veterans organizations and programs, which help transition military employees to non-military positions through training and education is the IA, IT and Cybersecurity fields..
e. Support to the National Guard Bureau to improve their ability to train and educate their IA/IT and Cybersecurity workforce.

1. **ANNEX II Technical Proposals**: (See Template also) In proposing support for capacity building activity, CAE technical proposals to ANNEX II must provide a clear statement as to which of the two focus areas they are addressing. The proposal must also clearly address the following:

a. The intellectual merit of the proposed activity.
b. The broader impacts resulting from the proposed activity to include articulating how the funding will benefit the students, the CAE, the community and/or the DoD.
c. The specific elements of the Scholarship Program that will be enhanced or strengthened by the requested support.
d. The impact to the Scholarship Program, the CAE and potentially the broader community if the support is not received.

[2] The use of "Virtual" labs and/or proven models is acceptable and desired for efficiency where appropriate (e.g. "Capture the Flag" and Cyber Defense type challenges, etc.)

2. **ANNEX II Cost Proposals**: Cost supporting ANNEX II should be identified separately from scholarship costs and should detail salaries, materials, equipment, and related direct and indirect costs for supporting the initiative(s) proposed. CAEs are advised that the request ***shall be limited to $125,000 or less in total.*** Only one proposal per focus area may be submitted.

II. EVALUATION CRITERIA

The ANNEX II "Proposal for Institutional Capacity Building" will be evaluated separately from the rest of the CAE's proposal package using the following criteria.

A. The merits of the proposed capacity building initiative(s) and their contributions to laying a strong foundation for the IASP are fully described. The elements of the program should be clearly articulated; and the institution must have a defined process to promote the IASP to its students and deliver high quality scholarship candidates (if applicable).

B. The CAE's current academic programs and proposed enhancements provide significant benefits to potential IA Scholarship students and support DoD mission needs. The CAE should identify key activities (e.g., programs, forums or partnerships with DoD, other government agencies, academia or private industry that enhance its cybersecurity academic credentials and contribute to faculty, staff, and student awareness and experiences in current cybersecurity trends. Requested research funding should align with DoD areas of interest and provide meaningful learning opportunities for both faculty and IASP students. Lab activities and curricula enhancements should provide students with critical cyber skills and knowledge. Diversity of student population and potential scholarship applicants should be supported through student demographics and partnerships with historically under-represented colleges and universities.

C. The costs of the proposal have been clearly articulated. Cost summations should be provided for 1) Total Funding Request for the Proposal; 2) Funding Request per Initiative. Additionally, each initiative must have costs identified for each relevant cost category (labor, equipment, travel, etc.). Estimates should be provided for single equipment purchases over $5K. All costs are realistic and reasonable.

D. There are factors that will reduce the total evaluation score (if applicable). Those factors are:

1. **Failure** to provide adequate administrative and/or academic support to current IASP students enrolled at the CAE institution.
2. **Failure** to properly invoice for previous IASP funding received.
3. **Failure** to submit annual DoD IASP Grant Reports as required.

III.TIMELINE

All Annex II proposals must must be part of the larger university scholarship proposal and

postmarked on/before Wednesday, May 31, 2017.

ATTACHMENT A

DoD IASP Proposal Preparation Instructions

PROPOSAL FORMAT

All proposals must consist of a technical proposal and a cost proposal. Proposals must adequately describe the technical objectives and approaches, impact on the Area of Interest (identified in Section 1.2), and requested expenditures. All submissions will be evaluated by technical reviewers in accordance with the evaluation criteria during the selection process.

1. The proposal must be clear, readily legible, and conform to the following requirements:
   a. Use one of the following typefaces identified below:
      i. Arial, Courier New, or Palatino Linotype at a font size of 10 points of larger
      ii. Times New Roman at a font size of 11 points or larger
      iii. Computer Modern family of fonts at a font size of 11 points or larger
      iv. NOTE: A font size of less than 10 points may be used for mathematical formulas or equations, figure, table or diagram captions and when using a Symbol font to insert Greek letters or special characters. PIs are cautioned, however, that the text must still be readable;
   b. No more than 6 lines of text within a vertical space of 1 inch; and
   c. Margins, in all direction, must be at least an inch.
   d. Digital signatures where applicable are acceptable.

2. The proposal will consist of the following documents in this order.
   a. Proposal Cover page (see template A) (one page)
      i. Title of proposal submitted in response to the ***NAME OF SOLICITATION***
      ii. Name, Title, Contact Information and Signature of the Principal Investigator (PI) or Project Director (PD):
      iii. Name and Title of the University Official authorized to obligate contractually and with whom business negotiations should be conducted:
      iv. Current federal or DoD grants, identify the Agency, Point of Contact, Phone Number, and amount.
   b. Proposal Summary: (continuation of the Proposal Cover Page Template A) (one page)
      i. Funds Requested:
         1. Recruitment Scholarship
         2. Capacity Building
         3. Total
      ii. Required Grant Start Date / Fall Semester Start Date
      iii. Indicate proposed partnership with another institution, and if the proposed partner is a minority institution. The U. S. Department of Education reference for minority institutions is located at: http://www2.ed.gov/about/offices/list/ocr/edlite-minorityinst-list-tab.html and the United States code 20 U.S.C. 1067k refers to the term "minority institution" as an institution of higher education whose

enrollment of a single minority or a combination of minorities include: American Indian, Alaskan Native, Black (not of Hispanic origin), Hispanic (including persons of Mexican, Puerto Rican, Cuban, and Central or South American origin), or Pacific Islander.

iv. Provide a copy or link to the most recent A-133 Single Audit Report: All non-Federal entities that expend $750,000 or more of Federal awards in a year ($300,000 for fiscal year ending on or before December 30, 2003) are required to obtain an annual audit in accordance with the Single Audit Act Amendments of 1996, OMB Circular A-133, the OMB Circular Compliance Supplement and Government Auditing Standards. A single audit is intended to provide a cost-effective audit for non-Federal entities in that one audit is conducted in lieu of multiple audits of individual programs.

v. **Mandatory Required Codes / Registrations:**

1. **Provide a response for each**:
   - a. Taxpayer Identification Number (TIN)[1]
   - b. Data universal numbering system (DUNS)[2] Number
   - c. System for Award Management (SAM) https://www.acquisition.gov (printed copy of registration is acceptable)
   - d. Acquisition Resource Center Registration (ARC) http://www.nsaarc.net/Index (printed copy of registration is acceptable)
2. **Provide one or both**:
   - a. Federal Interagency Committee on Education Code (FICE)
   - b. Integrated Postsecondary Education System Code (IPEDS).

vi. Signature of the Authorized University Official **(use blue ink)** and the Date

c. Executive Summary (one page)

d. Table of Contents (one page)

e. Sign and attach - Certifications 201**7** (Attachment B)

f. Technical Proposal - Offerors shall mark their proposals to indicate the use of proprietary information and/or data. No more than 20 pages for each proposed project from Section 1.2 for a total of 120 pages. (6 projects @ 20 pages each – 120 pages total). Individual projects must be clearly identifiable within the proposal.

i. Recruitment Program + Student applications rank ordered

1. One file per student, not one continuous file for all students. Saved in PDF format with the following file name: ***LAST NAME_First Name_University***

ii. Capacity Building Proposals

g. Cost Proposal

i. Excel Spreadsheet Cost (Attachment E)

[1] The DoD is required by 31 U.S.C. 7701 to obtain each recipient's Tax Identification Number (TIN) (usually the Employer Identification Number) for purposes of collecting and reporting on any delinquent amounts that may arise out of the recipient's relationship with the Government.

[2] The institution's number in the data universal numbering system (DUNS) is a unique nine digit (all numeric) identification number for organizations. Dun & Bradstreet Corporation assigns it. You can receive a DUNS number by calling Dun & Bradstreet at 1(800) 333-0505 or go to the Dun & Bradstreet Web site at https://eupdate.dnb.com/requestoptions.html?cm_re=Homepage*Resources*DUNSNumberLink

ii. Offerors will submit a separate written cost proposal for the recruitment student program and the capacity building project. No page limit on written cost proposal.

iii. Standard Form-424A Budget Information – Non-Construction Programs. (Attachment X)

h. CVs / Resumes are limited to 5 pages per faculty member and do not count towards the technical proposal page limits.

i. Submission Format- 31 May 2017: Proposal may be email AskIASP@nsa.gov or sent via hard copy. For those that email the application, official transcripts must follow via hard copy.

DEADLINES

Institutionally approved, signed, completed proposals which include all items listed above and all student applications must be **postmarked or emailed on/before Wednesday, 31 May 2017**. The entire proposal, containing all items listed above is to be mailed to:

DoD IASP National Security Agency
Attn: A233, NIETP, Suite 6804
9800 Savage Road
Fort George G. Meade,
MD 20755-6804

For emailed proposals please provide official transcript by mailing them via the USPS to the address above or by Commercial Courier to the address below!

If you are having the package sent via commercial courier (FedEx, UPS, DHL, etc.), the package shall be delivered to the following address (**DO NOT HAND DELIVER** TO THIS ADDRESS OR TO 9800 SAVAGE ROAD):

NSA
1472 Dorsey Road, Door 1, 2 or 3
Hanover, MD 21076-6744
Attn: DoD IASP, A233 Suite 6074
Phone: (410) 854-6206

LATE SUBMISSIONS

The CAE is responsible for submitting the proposal and student materials to the DoD IASP Program Office at the National Security Agency by the date and time specified.
Proposals or student materials that are postmarked after the deadline of 28 February 2017, are "late" and will not be considered for an award or scholarship

INCOMPLETE SUBMISSION

Proposals or student materials submitted in the wrong format, using wrong forms, or missing items will be deemed incomplete and will not be considered for an award of scholarship program selection.

CERTIFICATIONS REGARDING LOBBYING; DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS; AND DRUG-FREE WORKPLACE REQUIREMENTS

Applicants should refer to the regulations cited below to determine the certification to which they are required to attest. Applicants should also review the instructions for certification included in the regulations before completing this form. Signature of this form provides for compliance with certification requirements under 34 CFR Part 82, "New Restrictions on Lobbying," and 34 CFR Part 85, "Government-wide Debarment and Suspension (Nonprocurement) and Government-wide Requirements for Drug-Free Workplace (Grants)." The certifications shall be treated as a material representation of fact upon which reliance will be placed when the Department of Education determines to award the covered transaction, grant, or cooperative agreement.

1. **LOBBYING**

As required by Section 1352, Title 31 of the U.S. Code, and implemented at 34 CFR Part 82, for persons entering into a grant or cooperative agreement over $100,000, as defined at 34 CFR Part 82, Sections 82.105 and 82.110, the applicant certifies that:

(a) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the making of any Federal grant, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal grant or cooperative agreement;

(b) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal grant or cooperative agreement, the undersigned shall complete and submit Standard Form - LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions;

(c) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subgrants, contracts under grants and cooperative agreements, and subcontracts) and that all subrecipients shall certify and disclose accordingly.

2. **DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS**

As required by Executive Order 12549, Debarment and Suspension, and implemented at 34 CFR Part 85, for prospective participants in primary covered transactions, as defined at 34 CFR Part 85, Sections 85.105 and 85.110--

A. The applicant certifies that it and its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;

(b) Have not within a three-year period preceding this application been convicted of or had a civil judgement rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

(c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in paragraph (2)(b) of this certification; and

(d) Have not within a three-year period preceding this application had one or more public transaction (Federal, State, or local) terminated for cause or default; and

B. Where the applicant is unable to certify to any of the statements in this certification, he or she shall attach an explanation to this application.

3. **DRUG-FREE WORKPLACE (GRANTEES OTHER THAN INDIVIDUALS)**

As required by the Drug-Free Workplace Act of 1988, and implemented at 34 CFR Part 85, Subpart F, for grantees, as defined at 34 CFR Part 85, Sections 85.605 and 85.610 -

A. The applicant certifies that it will or will continue to provide a drug-free workplace by:

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;

(b) Establishing an on-going drug-free awareness program to inform employees about:

(1) The dangers of drug abuse in the workplace;

(2) The grantee's policy of maintaining a drug-free workplace;

(3) Any available drug counseling, rehabilitation, and employee assistance programs; and

(4) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);

(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will:

(1) Abide by the terms of the statement; and

(2) Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;

(e) Notifying the agency, in writing, within 10 calendar days after receiving notice under subparagraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to: Director, Grants Policy and Oversight Staff, U.S. Department of Education, 400 Maryland Avenue, S.W. (Room 3652, GSA Regional Office Building No. 3), Washington, DC 20202-4248. Notice shall include the identification number(s) of each affected grant;

(f) Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph (d)(2), with respect to any employee who is so convicted:

(1) Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or

(2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;

(g) Making a good faith effort to continue to maintain a drug-free workplace through implementation of paragraphs (a), (b), (c), (d), (e), and (f).

B. The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant:

Place of Performance (Street address. city, county, state, zip code)

____

____

____

Check **[ ]** if there are workplaces on file that are not identified here.

DRUG-FREE WORKPLACE
(GRANTEES WHO ARE INDIVIDUALS)

As required by the Drug-Free Workplace Act of 1988, and implemented at 34 CFR Part 85, Subpart F, for grantees, as defined at 34 CFR Part 85, Sections 85.605 and 85.610-

A. As a condition of the grant, I certify that I will not engage in the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance in conducting any activity with the grant; and

B. If convicted of a criminal drug offense resulting from a violation occurring during the conduct of any grant activity, I will report the conviction, in writing, within 10 calendar days of the conviction, to: Director, Grants Policy and Oversight Staff, Department of Education, 400 Maryland Avenue, S.W. (Room 3652, GSA Regional Office Building No. 3), Washington, DC 20202-4248. Notice shall include the identification number(s) of each affected grant.

As the duly authorized representative of the applicant, I hereby certify that the applicant will comply with the above certifications.

NAME OF APPLICANT	PR/AWARD NUMBER AND / OR PROJECT NAME DoD Informatoin Assurance Scholarship Program (DoD IASP)
PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	
SIGNATURE	DATE

The following will be included in any grant award:

MILITARY RECRUITING ON CAMPUS

As of 25 January 1995, DoD Grant and Agreement Regulations Part 23.1 “Military Recruiting on Campus” is to be added to DoD grants. The full text of the interim rule published in the Federal Register [at 60 FR 4544-4] is as follows:

“As a condition for receipt of funds available to the Department of Defense (DoD) under this award, the recipient agrees that it is not an institution that has a policy of denying and that it is not an institution that effectively prevents the Secretary of Defense from obtaining for military purposes: (A) entry to campuses or access to students on campuses; or (B) access to directory information pertaining to students. If the recipient is determined, using procedures established by the Secretary of Defense to implement section 558 of Public Law 103-337 (1994), to be such an institution during the period of performance of this agreement, and therefore to be in breach of this clause, the Government will cease all payments of DoD funds under this agreement and all other DoD grants and cooperative agreements, and it may suspend or terminate such grants and agreements unilaterally for material failure to comply with the terms and conditions of award.”

OMB Approval No. 0348-0040

ASSURANCES - NON-CONSTRUCTION PROGRAMS

Public reporting burden for this collection of information is estimated to average 15 minutes per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the Office of Management and Budget, Paperwork Reduction Project (0348-0040), Washington, DC 20503.

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the awarding agency. Further, certain Federal awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.

2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.

3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.

5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).

6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. §§1681-1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee-3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.

7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.

8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327-333), regarding labor standards for federally-assisted construction subagreements.

10. Will comply, if applicable, with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is $10,000 or more.

11. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the Endangered Species Act of 1973, as amended (P.L. 93-205).

12. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

13. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq.).

14. Will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported by this award of assistance.

15. Will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported by this award of assistance.

16. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

17. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."

18. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL	TITLE
APPLICANT ORGANIZATION	DATE SUBMITTED April 4, 2017

ATTACHMENT C
Department of Defense (DoD)
Information AssuranceScholarship Program (IASP)
Application Background
and
Requirements

CONTENTS

1. BACKGROUND

Cyberseucirty is considered so important to our national defense that a formal DoD IASP was established by the National Defense Authorization Act for 2001 (Public Law 106- 398). The purpose is to promote the education, recruitment, and retention of ***rising junior and senior undergraduate and graduate/doctoral students*** in cybersecurity studies.

The DoD is seeking rising junior and senior (third and fourth year) undergraduate and graduate/ doctoral students who are interested in full-ride scholarships for concentrated studies in cybersecurity. Students selected for the program will receive full scholarships. This requires the student to agree to serve one year of service to the DoD, upon graduation, for each year of scholarship received, in addition to the internship identified below. An opportunity also exists for scholarship payback through military service. Individuals choosing to enlist or accept a commission to serve on active duty in one of the Military Services shall incur a service obligation of a minimum of 4 years on active duty in that Service upon graduation. The Military Services may establish a service obligation longer than 4 years, depending on the occupational specialty and type of enlistment or commissioning program selected. Traditional Guardsmen and Reserve Soldiers are eligible to apply. Scholarship payback for this group is two-years of service for each year of scholarship recieved.

During breaks in their academic studies, Information Assurance Scholars will receive progressive, hands-on experience in information security internships. In return, scholars must agree to some restrictions and obligations regarding curriculum, GPA, and pre- and post-program employment. If all conditions are met, Information Assurance Scholars will receive full-time conditional/permanent positions in Components of the DoD upon program completion.

HOW TO APPLY

Only students at designated National Centers of Academic Excellence in Cyber Defense Education(CAE-CDE), National Centers of Academic Excellence Cyber Defense– Research (CAE-R), and National Centers of Academic Excellence – Cyber Operations, hereinafter referred to as CAEs may apply. Review the list of schools included with this announcement for clarification.

https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfml

Note: Students selected must attend full-time.

Review all application instructions and materials included with this announcement.

Pay close attention to the mandatory conditions of Financial assistance and employment.

Check with the identified Point of Contact for your college or university to find out what you must do to apply and to obtain an augmented application package if your school requires.one. (Application due dates and requirements may vary from school to school.)

Each CAE has designated a campus liaison, point of contact, or Principal Investigator (PI), for IASP management and administration. The above reference website provides known points of contact for the current CAEs. You are responsible for identifying the appropriate PI for the IASP On your campus.

DO NOT SUBMIT YOUR APPLICATION TO THE DOD. Submit your application package directly to the appropriate Point of Contact for your college or university.

2. DESCRIPTION OF SCHOLARSHIP AND EMPLOYMENT OPPORTUNITY

Chapter 112 of title 10, United States Code authorizes the IASP. The purposes of the program are to recruit and retain well-qualified personnel for work in the vital cybersecurity field and to cultivate continuing capacity for cybersecurity workforce development at select institutions of higher learning (CAEs) throughout the United States. As directed by the Secretary of Defense, the DoD CIO has delegated authority and responsibility to establish scholarship and institutional grant programs to achieve these purposes, including the authority to conduct civilian employee recruitment for these purposes. This program is executed by the National Information Assurance Education and Training Program (NIETP) of the National Security Agency (NSA) on behalf of the DoD.

Rising junior and senior undergraduates, master's and doctoral candidates, who are U.S. citizens and are at least 18 years of age are eligible for consideration for the programStudents selected as Information Assurance Scholars will receive the full cost of tuition, books (from the institution/ degree specific required book list, not books which are optional for the class), required fees (including health care), and a stipend to cover room and board. The stipend levels are $22,500 for undergraduate students and $30,000 for graduate (Master's/PhD) students. Disabled students may receive additional allowances. There are no allowances for dependents. Additional years of scholarship awards are dependent upon satisfactory academic progress, internship performance, if applicable, and the availability of funds. Returning students will be given first priority over new students to the program as long as they continue to meet the IASP requirements

[1] If a student is applying for only one half of a school year (or graduates 1 semester early), that student shall only receive half the stipend amount. The stipend is based upon an annual full-time attendance at the University. Students planning to graduate in December 2017,must be clearly identified (**for placement purposes**).

and appropriate funding is available. Scholarship recipients who successfully complete the terms of an initial one or two year scholarship (for example, complete an undergraduate degree), may apply for a second scholarship of up to three years for completing an advanced degree, if the sponsoring agency agrees. When funding allows, students may be provided funding to attend one cybersecurity related conference - USA-based only. No foreign travel authorized.

3. APPOINTMENT AND HIRING AUTHORITIES

Chapter 112, title 10, United States Code anticipates that recipients of scholarships will participate in experiential learning assignments (called "internships" in the law) at the DoD Components and Agencies while completing thier academic degree programs. There are a variety of hiring authorities acorss DoD and the determination will be made by those Agencies in conjunction wiht the IASP Program Office

Information Assurance Scholars will be appointed at those General Schedule grade levels for which they are qualified and selected by DoD component officials. Since the Area of Consideration for scholarship applicants includes rising junior and senior year undergraduates, master's and doctoral degree candidates, and graduate/doctoral certificate program s tudents, it is anticipated that applicants will (variously) meet minimum qualification standards for Student Trainee appointments at GS-0099-7, GS-0099-9, and GS-0099-11. The Military Departments and DoD Components that select and appoint students will decide at what grade levels successful Information Assurance Scholars will be appointed in light of any applicable component-unique factors such as the target occupations or full-performance position levels for the candidates. To obtain information on the general salary schedule, please visit:

https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/2017/general-schedule/

4. MINIMUM ELIGIBILITY FOR SCHOLARSHIP AND APPOINTMENT

To be eligible for the IASP opportunity described in this announcement, you must meet all of the following minimum requirements:

a. You must be 18 years of age or older.

b. You must be a citizen of the United States at the time of application. ***Note, if family members are not U.S. Citizens, some DoD Agencies may be unable to process the applicant (student) to the security clearance level required. Every effort will be made to assign eligible students at an Agency without such restrictions.***

c. You must be enrolled (or accepted for enrollment) in one of the identified CAE colleges or universities listed in this announcement, or enrolled (or accepted for enrollment) at an institution selected by a CAE as a collaborative partner for these purposes.

d. You must have completed (or by August 2017 will have completed) at a minimum the first two years of an undergraduate degree program and be eligible to (a) begin either the third or fourth year of an undergraduate degree program; (b) begin the first or second year of a Master's degree program; or (c) pursue doctoral studies

e. You must be pursuing a course of study and/or have a declared major in one of the scientific, technical, or managerial disciplines related to cybersecurity or with a concentration in cyber security.

For these purposes, the scientific, technical and managerial disciplines related to computer and network security and cybersecurity are:

i. Biometrics
ii. Business:
    1. Management
    2. Administration
    3. Process Analysis
iii. Computer:
    1. Crime Investigations
    2. Engineering
    3. Forensics
    4. Information Science
    5. Information Systems
    6. Programming
    7. Science
    8. Systems Analysis
iv. Critical Information Infrastructure Assurance
v. Cyber:
    1. Operations
    2. Security
    3. Policy
vi. Cryptography
vii. Database Administration
viii. Data Management
ix. Digital and Multimedia Forensics
x. Electrical Engineering
xi. Electronics Engineering
i. Information Assurance:
    1. Systems and Product Acquisition
    2. Training, Education and Management
xii. Information Security (Assurance)
xiii. Information Systems
xiv. Information Technology:
    1. Acquisition
    2. Program/Project Management
xv. Mathematics
xvi. Network Administration and Operations
xvii. Network Management
xviii. Operation of Computer Emergency Response Teams
xix. Software Engineering
xx. Systems Security Engineering
ii. Threat and Vulnerability Assessment, to include Risk Management
iii. Web Security
iv. And other similar disciplines as approved by the DoD Chief Information Office (DoD CIO).

See the web page information below, which provides more information about fulfilling the necessary security requirements. Failure to be able to obtain a security clearance is grounds for dismissal from the DoD IASP. You must be able to obtain the required security clearance for the position selected. **You may be required to undergo certain tests, including drug and polygraph tests, to obtain and maintain a clearance. Before you may be awarded a scholarship or hired by DoD, you will be required to complete certain forms to initiate the security clearance process.** Some of these forms will require that you reveal extensive information about your background, such as potentially sensitive information about your financial circumstances and any arrests and/or convictions for offenses of any kind. You must agree to all of these conditions of employment and you must complete these forms as a condition of financial assistance and appointment.

i. *Current web pages from the Office of Personnel Management (OPM) are provided below. These are provided for your review and consideration in determining whether you will be eligible for a security clearance. They may not be all inclusive, however, it is highly recommended that you review and understand the requirements prior to signing up to participate in the DoD IASP.*

https://www.opm.gov/investigations

5. ACADEMIC SUFFICIENCY

Your school must recommend you for scholarship. The CAE shall review the application materials, and conduct such verification as may be necessary to establish the following standards of academic sufficiency. CAEs shall exclude from further evaluation (and provide an endorsement of "Not Recommended" for) any applicant unable to meet the following academic requirements:

a. The applicant is pursuing a course of study and/or has a declared major in one of the scientific, technical or managerial disciplines related to computer and network security that are enumerated under Section 4.E. above.

b. As an undergraduate student, the applicant has a 3.2 out of a 4.0 grade point average *(GPA)* or, as a graduate student, the applicant has a 3.5 GPA out of 4.0, or an analogous rank based on a comparable scale.

c. The applicant's demonstrated potential for academic success and fulfillment of degree requirements is substantial. CAEs shall review the factors enumerated below, and shall exclude from further evaluation and not recommend any candidate unable to achieve a minimum score of 2 points on a 5-point scale. Scale values range from Insufficient Potential (One), Sufficient Potential (Two), Average Potential (Three), High Potential (Four), and Superior Potential (Five). Factors to be considered in arriving at the rating for "demonstrated potential" are:

- The applicant's original transcript(s) from all institutions of higher education attended
- The applicant's current Grade Point Average (GPA)
- Academic honors, distinctions and awards
- Letters of reference

6. KNOWLEDGE AND ABILITY

Please use Attachment E, Student Endorsement and Ranking Form, for the following**: The CAE shall document its evaluation of each applicant meeting administrative and academic sufficiency**

requirements against the following competencies, using a 5-point scale of values, to assess and report on *each* of the six competencies below. The rating scale is:

- No Knowledge or Ability (One)
- Basic Knowledge or Ability (Two)
- Intermediate Knowledge or Ability (Three)
- Advanced Knowledge or Ability (Four)
- Superior Knowledge or Ability (Five)

Evaluations of the following factors shall be based on the supplemental application material provided by the candidates, letters of reference, and any additional information provided by the applicant in response to CAE requests made for this purpose.

- Knowledge of the techniques of the information technology and/or information security (assurance) discipline, including encryption, access control, physical security, training, threat analysis, and authentication.
- Knowledge of the human factors in the information technology and/or information security (assurance), including human computer interaction, design, training, sabotage, human error prevention and identification, personal use policies, and monitoring.
- Ability to identify and analyze problems, distinguish between relevant and irrelevant information to make logical decisions, and provide solutions to individual and organizational problems.
- Ability to consider and respond appropriately to the needs, feelings, and capabilities of different people in different situations; is tactful, compassionate and sensitive, and treats others with respect.
- Ability to make clear and convincing oral presentations to individuals or groups; listens effectively and clarifies information as needed, facilitates an open exchange of ideas and fosters an atmosphere of open communication.
- Ability to express facts and ideas in writing in a clear, convincing and organized manner appropriate to the audience and occasion.

The CAE shall also provide in written paragraph form the reason for one of the following recommendations:

- Highly Recommended
- Recommended
- Not Recommended

7. GENERAL INFORMATION

Application Forms and Materials

On the application and the following pages you will find instructions for preparing and submitting an application for the IASP, as well as application forms and materials. Please read all information and instructions for application preparation before you begin. The application itself consists of your resume and all of the OF612 supplements. **The OF612 Supplemental Competency Statement and Resume must be included or the package will be deemed non-responsive and will not be considered**.

Please be aware that your CAE is required by the DoD to participate in the evaluation of your application for scholarship assistance under this program. Your CAE may fulfill its responsibilities to evaluate your application in a variety of ways. Your CAE might constitute a panel to review your application materials or conduct interviews with you or other applicants. To fulfill its responsibilities, your CAE may require that you obtain and submit information and/or materials in addition to those required in the application package. Any written information or material that your CAE requires shall become the CAE Supplement to your OF612 and must be included in the final application package that your school transmits to the DoD in order for you to receive consideration.

Therefore, if you are interested in applying for this opportunity, ***you should check with the PI, for your school immediately*** to learn of any additional application requirements.

Veteran's Preference in Hiring

If you served on active duty in the United States Military and were separated under honorable conditions, you may be eligible for veteran's preference. For further details visit the Office of Personnel Management website at: http://www.opm.gov/veterans/html/vetguide.asp.

To claim 5-point veterans' preference, attach a copy of your DD-214, Certificate of Release or Discharge from Active Duty, or other proof of eligibility, to your Optional Form 612 - Optional Application for Federal Employment, as required at Item 15 of the application.

To claim 10-point veterans' preference, attach an SF 15, Application for 10-Point Veterans' Preference, plus the proof required by that form, to your Optional Form 612 - Optional Application for Federal Employment, as required at Item 15 of the application.

Applicants with Disabilities

You can find out about alternatives for submitting your application by calling the Office of Personnel Management at 912-757-3000. If you have a hearing disability, call TDD 912-744-2299. You may obtain case-by-case assistance by calling the Department of Defense point of contact for this announcement. The name, address, and email address of the point of contact for this announcement are below:

DoD IASP Program Office
National Security Agency
Attn: NIETP, A233, Suite 6804
9800 Savage Road
Fort George G. Meade, MD 20755-6804 AskIASP@nsa.gov

Equal Employment Opportunity

The Department of Defense is an Equal Opportunity Employer. All qualified persons shall receive consideration for this opportunity without regard to political, religious, labor organization affiliation or non-affiliation, marital status, race, color, sex, national origin, non-disqualifying physical disability, age, or sexual orientation.

8. OTHER IMPORTANT INFORMATION ABOUT THIS OPPORTUNITY

a. Before being hired, the appointing agency (the specific DoD Agency requesting to hire you) will ask you to complete a Declaration for Federal Employment or other agency or component specific form to determine your suitability for federal employment and to authorize a background investigation of your suitability. The agency will also ask you to sign and certify the accuracy of all the information in your application. If you make a false statement in any part of your application, you may not be hired; you may be fired after you begin work; or you may be fined or jailed.

b. You will be required to obtain and maintain eligibility for a security clearance in order to receive financial (scholarship) assistance or an appointment under the IASP. The appointing agency will ask you to complete certain forms to initiate the security clearance process. These forms require you to reveal many details about your background, including your financial circumstances, and other sensitive matters such as any arrests and/or convictions for offenses of any kind. You must complete these forms as a condition of financial assistance and appointment.

c. If you are a male over age 18 who was born after December 31, 1959, you must have registered with the Selective Service System (or have an exemption) to be eligible for a federal job.

d. Federal law prohibits officials from appointing, promoting, or recommending their relatives.

e. Federal annuitants (military and civilian) may have their salaries or annuities reduced. All employees must pay any valid delinquent debts or the employee's payroll office may garnish their salary.

9. APPLICATION CONTENT REQUIREMENTS

STUDENTS NOT CURRENTLY IN THE IASP: An acceptable application package for the IASP consists of the following requirements:

1. **The IASP Student Application** completely filled out and signed. (Attachment D)
2. **Separate sheet highlighting recognitions, honors and awards**. You may attach a separate sheet of plain 8 ½" x 11" paper on which you record your responses or the continuations of your responses. On each such page, indicate your name.
3. **Supplemental Academic Sufficiency Statement**. You must complete the Statement of Academic Sufficiency supplement to the OF612, to which you must attach the following additional supplemental statements:
    a. **Resume**
    b. **One (1) Letter of Reference** from a current faculty member who is fully knowledgeable of your potential for successful learning, your knowledge, and your ability. See remainder of application package for instructions about the content of this Letter of Reference. Letters must be on University letterhead and contain the full name and contact information of the faculty member (phone, email, and address).
    c. **One (1) additional Letter of Reference** from either a current or former faculty member, or a current or former supervisor who is fully knowledgeable of your potential for successful learning, your knowledge, and your ability. See remainder of application package for instructions about the content of this Letter of Reference. Letters must be on official letterhead and contain the full name and contact information of the faculty member or current/former supervisor (phone, email, and address).

d. **Official (certified)** transcripts from all the institutions of higher learning you have attended. **Web printed copies will not be accepted**.

e. **Supplemental Competency Statement: Knowledge, Skills and Attributes:** You must complete the OF612 Supplemental Competency Statement with narrative responses that describe the level of your attainment of the knowledge and ability factors indicated. See remainder of application package for instructions about the content of this supplemental statement.

f. **Signature of the Supplemental Statement of General Academic and Employment Conditions**. If you agree with the all of the academic and employment conditions required for your receipt of scholarship assistance and appointment under the IASP, and wish to be considered for it, you must sign the OF612 Supplemental Statement of General Academic and Employment Conditions, which is the last page of the Attachment D, Student Application.