Department of Defense
Cyber 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
which includes
National Centers of Academic Excellence in Cyber Defense Education and
National Centers of Academic Excellence – Research,
and
Universities designated by the National Security Agency
as
National Centers of Academic Excellence – Cyber Operations
(herein after referred to as CAEs)

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

Proposal Submission: 28 February 2019

SUBJECT TO AVAILABILITY OF FUNDS

CONTENTS

Application forms will be published on the following website:
https://www.iad.gov/NIETP/CAERequirements.cfm

I. INTRODUCTION

The Department of Defense (DoD) Cyber Scholarship Program (CySP) is authorized by Chapter 112 of title 10, United States Code, Section 2200. The purpose of the program is to support the recruitment of new cyber talent and the retention of current highly skilled professionals within the DoD cyber workforce. Additionally, this program serves to enhance the national pipeline for the development of cyber personnel by providing grants to institutions of higher education.

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 Education (Cyber Defense or Research) and/or designated 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 cyber-related disciplines for Academic Year 2019- 2020. CAEs may propose collaboration with other accredited institutions, and are encouraged to include accredited post-secondary minority institutions. CAEs must be in good standing with the CAE Program Office and not be delinquent on any required documentation by the CAE Program Office. CAEs may also propose to undertake a special partnering agreement with the College of Information and Cyberspace (CIC) of the National Defense University (NDU). [Special note: Proposal requirements for addressing the CIC/NDU partnership options are described in ANNEX I and should be responded to in a separate ANNEX I submission.]

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 cyber-related topics to providing a strong foundation for a Cyber 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 recruitment scholarship program during the Academic Year 2019-2020, students falling into one of the following categories may apply:

- Rising second-year CAE Community College (pilot program) students who will be transitioning into a bachelor's degree program at a 4-year CAE
- Juniors, Seniors pursuing a bachelor's degree (Sophomore's promoting to a Junior in Fall 2019 are eligible to apply)
- Students in their first or second year of a master's degree; or
- Students pursuing doctoral degrees.

Application retention/ANNEX I scholars apply directly through their DoD Agency / Component. CAEs are not required to forward their applications.

II. TERMINOLOGY

A. DoD Cyber Workforce*:* For purposes of this program, the term DoD cyber workforce refers to personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel

assigned to the areas of cyber effects, cybersecurity, cyber IT, and portions of the intelligence workforces. The four workforce categories are:

- **Cybersecurity workforce**. Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.

- **Cyber Effects workforce**. Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

- **Cyber IT workforce**. Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT, as well as information resource management; and the management, storage, transmission, and display of data and information.

- **Intelligence workforce (cyber).** Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

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

C. Relevant cyber-related academic disciplines, with concentrations in cyber security, would include, but are not limited to:
    - Biometrics
    - Business:
        a. Management
        b. Administration
    - Computer:
        a. Crime Investigations
        b. Engineering
        c. Forensics

    d. Information Science
    e. Information Systems
    f. Programming
    g. Science
    h. Systems Analysis
- Critical Information Infrastructure Assurance
- Cyber:
    a. Defense
    b. Operations
    c. Security
    d. Policy
- Cryptography
- Database Administration
- Data Management
- Data Science
- Digital and Multimedia Forensics
- Electrical Engineering
- Electronics Engineering
- Information Assurance
- Systems and Product Acquisition
- Information Security (Assurance)
- Information Systems
- Information Technology:
    a. Acquisition
    b. Program/Project Management
- Mathematics
- Network Administration and Operations
- Network Management
- Operation of Computer Emergency Response Teams
- Software Engineering
- Systems Security Engineering
- Threat and Vulnerability Assessment, to include Risk Management
- Web Security
- Any other similar disciplines as approved by the DoD Chief Information Office (DoD CIO).

III. OVERVIEW OF PROGRAM SCOPE

The key elements of the DoD CYSP, 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. ***Recruitment / Basic Scholarships - Academic Year 2019-2020.*** The DoD estimates awarding scholarships (via grant awards) for a period of one year (beginning with the fall 2019 semester) to designated CAEs, operating independently or in collaboration with other accredited institutions, including accredited postsecondary minority institutions. The purpose is to lay a sound foundation for the development of a robust cyber program for undergraduate and graduate students enrolled in the CAE or its collaborating institutions' degree and graduate certificate cyber 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 a scholarship program within the university, CAEs may also request funds for capacity building activities. Grant awards are contingent upon availability of funds.

B. ***Retention / Annex I Scholarships – Academic Year 2019-2020***

1. *College of Information and Cyberspace (CIC) /NDU Partnership*: CAEs wishing to partner with the CIC/NDU will be required to accept the DoD civilian employees and military officers into their graduate degree programs, who have successfully completed the CIC graduate level CIO Certificate Program with a cybersecurity concentration. Requirements for addressing the CIC/NDU Partnership option are described in ANNEX I, and are to be responded to in separate ANNEX I Technical and Cost Proposal submissions. Administrative costs allowed for the program should include a visit to the CIC, for one overnight if necessary (if you are not in the local area). Additionally, if you do not currently have CIC partnerships students, please provide prices for a per student option, with a breakout of in-state/out-of-state (as applicable), MS and PhD (if both), and indicate the maximum number of partnership students you can accept during each year. Those with current partnership students must also address the necessary continuation costs for them. The requirements for the student application nomination and review process described below and in the accompanying Student Application materials for this program ***do not apply to current DoD/Federal civilian employees or military personnel*** whose applications for this program will be handled directly by the Department of Defense as described in ANNEX I.

2. ***Community College Scholarships (Pilot Program)***: Active duty military members, Reservists, National Guard members, as well as permanent DoD civilian employees seeking to enhance their cyber skills and knowledge may pursue an associate's degree at a community college designated as a National Center of Academic Excellence in Cyber Defense. Students must already possess a bachelor's degree in any field. A list of those institutions can be found at: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm. Community College CAEs who do not currently have such students should provide an estimated price per student (See Excel Spreadsheet – Attachment E), with a breakout of in-state/out-of-state (as applicable), and indicate the maximum number of students you can accept during each year. The requirements for recruitment student nominations and review described below and in the accompanying Recruitment Student Application ***do not apply to current DoD/Federal civilian employees or***

military personnel whose applications for this program will be handled directly by the Department of Defense as described in ANNEX I.

C. ***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 cybersecurity research and education in cyber-related disciplines 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 cyber and cybersecurity as they relate to the extended community and DoD. Two focus areas are DoD Partnerships and Outreach to Technical Colleges, Community Colleges, and/or Minority Serving Institutions. Details for all activities will be described in ANNEX II. CAE requests for capacity building support should be part of the overall institutional submission, but identified in the "how" section of the submission. Narratives for the scholarship and capacity building portions should be severable from each other

D. ***Proposal Formats*****: Attachment A Identifies Proposals Formats:** At a minimum, the proposal must respond to either the establishment/continuation of a Cyber Scholarship Program (Recruitment / Basic), the establishment/continuation of a Cyber Scholarship Program (Retention/Annex I). One of both scholarship options must be submitted as part of the proposal in order to be eligible for any ANNEX II/Capacity Building opportunities.

E. ***The DoD CySP Application Due Dates***: CAEs electing to submit a proposal to establish a recruitment/basic scholarship program must establish a due date for student scholarship applications that will allow sufficient time to evaluate student applicants and prepare recommendations of student candidates for postmarking or emailing on/before **Thursday, February 28, 2019**. These dates are critical in order to ensure grant awards prior to August 1, 2019 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:*** CAEs are required to provide an assessment of each recruitment applicant. Assessment of retention applicants will be handled by the nominating DoD Agency/Component. The actual selection of student scholars will be made by DoD evaluators for both programs.
   1. ***Recruitment / Basic Scholarships***: Students selected as Cyber 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 $20,000 for community college students (pilot program), $25,000 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 into DoD employment.
   2. ***Retention / Annex I Scholarships***: Students selected as Cyber 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, and potential travel for degree specific degree

events. Retention Scholars will continue to receive their DoD/Military pay and will be required to perform a service obligation to their parent agency/component.

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.
   1. ***Recruitment / Basic Scholarships***: 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.
   2. ***Retention / Annex I Scholarships***: Returning students will not be required to re-apply but must show progression in their degree program at the required GPA levels (3.0 in a bachelor's degree for those pursing the community college option and a 3.2 for graduate programs (National Defense University, Air Force Institute of Technology, Naval Postgraduate School.)

IV. RECRUITMENT / BASIC STUDENT OBLIGATIONS

Students selected to participate in the DoD CySP 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. 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 CySP 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.

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.

Community College (pilot program) and 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 CySP 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 $5,500 in an academic year, a student may not accept simultaneous remuneration from another scholarship or fellowship. The DoD CySP is a first pay scholarship program.

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. RETENTION / ANNEX I STUDENT OBLIGATIONS:

Students selected to participate in the DoD CySP will be required to sign a written agreement obligating them to work for the DoD. Additional information about obligations can be found in the "Guidelines for DoD Civilians and Military Personnel Academic Opportunities for Calendar Year 2019 and 2020.

VI. 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. Addressed below in paragraph VII below are the specific requirements for advertising the scholarship among the candidate student populations, collecting and assessing student applications, and reporting on the process. Proposal evaluation criteria will review how well CAEs conduct the recruitment and assessment process.

VII. CAE ROLE IN RECRUITING AND ASSESSING SCHOLARSHIP CANDIDATES

If a CAE decides to participate in the recruitment/basic scholarship program, 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 CySP opportunity:
   - 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 CySP opportunity.
   - Publish and ensure that all appropriate DoD CySP 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 CySP.

B. ***Managing the Application Review and Candidate Assessment Process***: CAEs electing to propose establishment of a recruitment/basic 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.
   - 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 Cyber Scholarship Application Background and Requirements. ***Current DoD/Federal Employees, Active Duty Military/Reserves/Guard, or students with an existing service obligation are not eligible to apply for the recruitment/basic scholarship***
   - 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. In addition to a brief statement about each student, CAEs shall indicate only one of the following **three levels** of endorsement for each applicant:
     i. **Not Recommended**
     ii. **Recommended**
     iii. **Highly Recommended**

C. ***Submitting Student Scholarship Applications and CAE Review and Endorsement***: CAEs that propose to support the recruitment/basic 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.

VIII. TECHNICAL PROPOSALS

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

IX. COST PROPOSALS

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

X. GRANT PROPOSAL EVALUATION CRITERIA AND SELECTION PROCESS

A. Recruitment/Basic Student Applications: Applications will be reviewed by the DoD CySP Program Office for eligibility. Once eligibility is determined, a copy of all student applications in the highly recommended and recommended category will be provided to the hiring DoD Agencies for review. Each agency will review applications based on the rules and policies that govern their agency.

B. Overall Proposals: Proposals will be evaluated by a panel of Department of Defense cyber professionals 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:

- The merits of the institution's proposed approach to designing and developing a robust CyberScholarship Program and the likelihood of its producing the highest quality Cyber Scholars for the DoD employment.
- The quality of the institution's process for promoting and advertising the CySP 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.
- The proposed program's congruence with statutory intent, the requirements of the DoD, and its relevance and potential contribution to the DoD mission needs.
- The qualifications of key faculty, staff and advisors, and their proposed role in the scholarship program.
- The adequacy of the institution's existing resources to accomplish the program objectives.
- The realism and reasonableness of the cost proposal.

C. Capacity Building Proposals: Proposals will be evaluated by a panel of Department of Defense cyber professionals 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: (Criteria is also addressed in ANNEX II Institutional Capacity Building)

1. ***Sound & Reasonable Methodology*** - Institution demonstrates a sound method for achieving the stated goals. A timeline of activities is included.
2. ***Benefit to the CAE***: Institution demonstrates a clear benefit to the CAE.
3. ***Development Opportunities***: Institution demonstrates or outlines development opportunities for faculty and students of the CAE.

4. ***Benefit to the CAE Network and Cybersecurity Education***: Institution includes a plan to disseminate results of the proposed project to strengthen the Cybersecurity Education programs within and outside of the CAE network.
5. ***Student Interaction***: Institutions describes how students will play an active role in the project.
6. ***Identified Partners***: Institutions provide contact information for project partners or those who will benefit from the project.
7. ***DoD Partnerships***: Proposal should support key DoD priorities, including but not limited to: artificial intelligence and cybersecurity, cloud computing, mobile technology, or other emerging needs as well as military organizations and support groups.
8. ***Outreach to Minority Institutions***: Proposals should include the development of meaningful, sustainable, results-oriented partnerships; or collaborations with minority institutions.
9. **Project Innovation**: Institution describes how this project is innovative.
10. **Costs**: Institution describes how the costs are reasonable in proportion to the scope of the proposal.

XI. AWARDS

Recruitment Scholarship notifications for students will be announced to the CAEs in the May 2019 timeframe. The grants will be awarded in the July 2019 timeframe. Awards will be made for one year only. Based on scholarship selections, the DoD may award a lower level of funding than what was 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 may not be selected in the competition for scholarship and DoD appointments. 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:

- *Telephone:* 1-866-606-8220;
- *SAM Website:* 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. ACQUISITION RESOURCE CENTER (ARC)

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 solicitation. The offeror 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. ELECTRONIC INVOICING:

Effective 2018 January 1, per 17(b) of the standard Terms and Conditions incorporated into all grants, invoices must be submitted electronically through the Maryland Procurement Office (MPO) website. Invoice submission through the MPO website is **MANDATORY** for organizations that have

grants with National Security Agency (NSA). Grantees must have a current PKI Certificate to utilize this function. Hardcopy invoice will no longer be accepted after this date. Be advised that hardcopy invoices will be rejected unless otherwise approved by the Office of Contracting and Accounts Payable.

Access to the MPO website requires an External Certificate Authority/Interim External Certificate Authority (ECA/IECA) PKI Certificate. Information on purchasing an ECA/IECA Certificate, including its initial and annual cost, is available on the internet at: http:// iase.disa.mil/pki/eca (must be a Medium Assurance Certificate). The grantee shall contact the Electronic Commerce Office at (410) 854-5445 if they need additional information. After obtaining the ECA/IECA certificate, the grantee must contact the Electronic Commerce Office to obtain an account if one does not currently exist.

Steps for Obtaining a PKI and Instructions for Invoicing Electronically:

- Obtain an ECA Medium Assurance Certificate through either ORC, Identrust, or DoD. Certificates come in three forms either software (browser based), token (preloaded USB device), or hardware (CAC card loaded). It is the grant awardee's preference what form of the ECA certificate that is chosen. Costs range from $100 - $300 (per year). This process normally takes one to one-and-a-half weeks to receive the certificate. Costs may be charged as a direct or indirect cost. No additional funds will be allocated to the grant as a result of this action.
- Once the certificate is received, contact the MPO Help Desk to request an account.
- Contact can be via email at dialogue@ec.ncsc.mil or phone at (410) 854-5445. It takes about 20-25 minutes to create the account.
- You will receive a welcome email entitled *Welcome to the MPO Website* that includes the user ID, password, and instructions on getting started.
- The MPO Help Desk can provide any detailed support needed for access and submission of electronic invoices through MPO.
- Invoices MUST be submitted using Standard Form SF270 as 300 dpi black and white .TIF using Group IV compression or as 300 dpi black-and-white .PDF images. Invoices shall be legible, quality, un-skewed images. Invoices shall not contain smudges, markings, shading, writing, stamps, annotation, coffee rings, highlighted data, circling, or redacted data.

XV. 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 Thursday, 28 February 2019**

XVI. LATE SUBMISSIONS

The CAE is responsible for submitting the proposal and student materials to the DoD CySP 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 2019** are "late," and will **not** be considered for an award or scholarship.

XVII. 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.

XVIII. CONTACT INFORMATION

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

DoD CySP Program Office
9800 Savage Road (Attn: A233)
Fort George G. Meade, MD 20755-6804
410-854-6206
e-mail: askiasp@nsa.gov

Department of Defense
Cyber Scholarship Program

Retention Scholarship Program

ANNEX I

Guidelines for DoD Civilian and Military Personnel Academic Opportunities for Calendar Years 2019 and 2020

CAEs *may, but are not required to,* address this section of the solicitation with a separate ANNEX I to their proposals titled "Proposal for Annex I – Retention Scholarships."

I. OVERVIEW

In addition to students who are not employed by the DoD at the time of application, the DoD will award a number of scholarships to current DoD employees to pursue degrees in cyber–related disciplines. Active duty military members (including active duty reservist and National Guard members), as well as permanent DoD civilian employees are eligible to apply, but must first be nominated by their Component. Nominated personnel shall be high performing employees who are rated at the higher levels of the applicable performance appraisal system and demonstrate sustained quality performance with the potential for increased responsibilities. Scholarship applicants must meet all requirements for acceptance to the specific institution they plan to attend. All eligibility criteria, especially academic credentials, should be carefully reviewed, as CySP requirements may be more stringent than general academic enrollment criteria for a particular college/university. No waivers will be granted.

A. Partnership with National Defense University's, College of Information and Cyberspace (CIC/NDU): DoD civilian employees and military officers who wish to pursue a full-time or part-time master's degree or doctorate in a cyber-related discipline. Applicants are nominated to enter the program in September 2019 or January 2020. Selected students will complete or have completed the first part of their degree through the NDU CIC and then enter a Partner University to complete the remaining degree requirements.
    a. CIC/NDU invites CAEs to propose partnerships or cite existing agreements that would articulate the CIC program with a follow-on opportunity at the CAE. This partnership would allow DoD students to complete a master's or doctorate with a concentration in cybersecurity. The following conditions will apply to a partnership arrangement between a CAE institution and CIC, and should be addressed in the ANNEX I proposal.
    b. DoD Student Population: DoD students who have completed a non-master's CIC program within the last four years may apply to begin a master's degree program at a designated partner university. DoD students who completed a master's degree CIC program may apply to begin a PhD program at select partner institutions.
    c. DoD Student Demographics: DoD students will be civilian employees or military officers at senior career levels (GS-12 and 0-4 officer rank and above) who are

competitively selected to participate in the DoD scholarship program.. Candidates should, at a minimum, possess an undergraduate degree and will be eligible to begin the first or second year of a master's degree program or doctoral studies.

B. Community College Scholarships (Pilot Program): Active duty military members, Reservists, National Guard members, as well as permanent DoD civilian employees seeking to enhance their cyber skills and knowledge may pursue an associate's degree at a community college designated as a National Center of Academic Excellence in Cyber Defense. A list of those institutions can be found at: https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

   a. Community College CAEs who do not currently have such students should provide an estimated price per student (See Attachment E - Excel Spreadsheet), with a breakout of in-state/out-of-state (as applicable), and indicate the maximum number of students you can accept during each year. The requirements for recruitment student application nomination and review and the accompanying Student Application do not apply to current DoD/Federal civilian employees or military personnel whose applications for this program will be handled directly by the Department of Defense.

II. ANNEX I Technical Proposals

CAEs must be willing to consider acceptance of DoD-selected students who have, at a minimum, an undergraduate degree and who meet all CAE university entrance requirements.

1. ***NDU Partnerships***: Once admitted to their graduate programs in a cyber related degree, partnering CAEs agree to award a minimum of nine (9) to fifteen (15) graduate credits from the designated CIC program. CAEs should indicate their willingness to accept these conditions or cite existing agreements, address the specific number of graduate credits they award or will award for the CIC programs. In addition, they should briefly address:
   a. number of students they can accommodate;
   b. master's and/or doctoral degree programs the students could participate in
   c. For **each** identified degree, provide the following information:
      a) number of additional credit hours required for degree completion
      b) estimated number of months to complete degree (do **not** include CIC time);
      c) prerequisite qualifications required or desired (if any) of potential DoD students;
      d) anticipated curriculum content of graduate programs proposed for the DoD students; **and**
      e) whether students will be required to attend courses on the college campuses or whether there are alternative means (e.g. web-based or satellite-based distance learning) through which students might participate in the CAE's degree programs.
      f) whether students will be eligible to attend courses part-time.
2. ***Community College Scholarships***: CAEs should briefly address the following:
      a) number of credit hours required for degree completion
      b) estimated number of months to complete degree;

c) prerequisite qualifications required or desired (if any) of potential DoD students;
d) whether students will be required to attend courses on the college campuses or whether there are alternative means (e.g. web-based or satellite-based distance learning) through which students might participate in the CAE's degree programs.
e) whether students will be eligible to attend courses part-time.

III. ANNEX I Cost Proposals:
CAEs wishing to partner with DoD in this effort should provide a separate cost ANNEX I in support of their "Proposal for Annex I – Retention Scholarships." In preparing this cost ANNEX I, CAEs should estimate the per student scholarship costs (e.g., tuition, books, and select academic fees) for DoD students. Unlike non-DoD (recruitment) students participating in the scholarship program, DoD students will not receive stipends. These scholarship costs should be identified separately from any other direct costs associated with the partnership proposed. Administrative costs allowed for the program should include a visit to the CIC/NDU, for one overnight if necessary ((if you are not in the local area) (only for those partnering with the National Defense University. Community Colleges are not eligible for this cost)). Additionally, if you do not currently have CIC partnership students, please provide prices for a per student option, with a breakout of in-state/out-of-state (as applicable), MS and PhD (if both), and indicate the maximum number of partnership students you can accept during each year. Those with current partnership students must also address the necessary continuation costs for them. In computing indirect (F&A) costs, CAEs are again reminded that F&A costs may not be applied to scholarship amounts per OMB Circular A-21. (http://www.whitehouse.gov/omb/circulars/a021/a21_2004.html#j).

V. EVALUATION CRITERIA

The "Proposal for Annex I – Retention Scholarships" ANNEX I will be evaluated separately from the rest of the CAE's proposal using the criteria below:

A. The merits of the CAE's proposed approach, and the ability of the institution to meet the conditions imposed by DoD for a CIC/NDU partnership or community college program.
B. The potential benefit of the program to DoD students and to meeting DoD mission needs.
C. The realism and reasonableness of the cost proposal.

Department of Defense
Cyber Scholarship Program

Institutional Capacity Building

ANNEX II

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 $6,000,000, may be set aside for capacity building for academic year 2019-2020.**

CAEs may submit one proposal which provides a response to one or both of the two focus areas identified below. The total proposal submission per CAE may not exceed $300,000.00 ($150,000.00 for each project). Any proposals exceeding this limit will be rejected. 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 cybersecurity research and education in cyber-related disciplines. In an effort to reduce redundancy and encourage collaboration, 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 cyber areas. 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 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. **Community Outreach:** Develop community outreach programs, such as partnerships with Wounded Warrior Project, Soldier for Life, and/or other veteran organizations and programs which help transition military members to non-military careers; K-12

STEM programs which lead to opportunities whit active duty military, Reserves, or National Guard.

d. **Curriculum Development:** Offers may propose to develop and deliver modular course materials.

   i. Proposals for curriculum development of these topics may take one of the following forms:

      1. Organize and run a curriculum-building workshop to develop and deliver cyber-related curricula in high need areas. Proposers should justify the proposed approach for building curriculum as well as the content area.
      2. Organize and run a clinic to teach a specific cybersecurity topic to teachers at the K-12 or university level. Proposers should justify the proposed model for the clinic to include why it will build educators' cybersecurity expertise as well as help them transition this knowledge to teaching practice.
      3. Curriculum must be made available to the DoD, NSA, and/or the CAE Community. Curriculum deliverables may include course syllabus and schedule for the course, teach materials, to include: recorded lectures, presentations, active-learning exercises, assessments and/or instructor notes/guidance. Courses should be developed in modules that can be used separately or in whole. Module - estimated completion time is more than 4 but less than 10 hours. Micro-module - estimated completion time is between 1-4 hours. Nano-module - estimated completion time is up to 1 hour. Developed curricula will be shared publicly so materials must be original work. Data rights sufficient to allow the government to exercise its rights under the terms and conditions of the grant are required. All delivered materials, documentation and information technology will meet the NSA ICT Accessibility Standards, derived from Section 508 of the Rehabilitation Act (29 USC 795d) and Web Content Accessibility Guidelines 2.0 AA requirements.

   ii. Topic areas:

      1. Supply Chain Risk Management
      2. Advanced Networking Security
      3. Artificial intelligence and machine learning as applied to cybersecurity
      4. Cybersecurity and Social Networks
      5. K-12 appropriate curricula
      6. Cellular – 4G/5G Mobile Systems Eco Systems (Defensive and Exploitation requirements)
      7. Security of embedded devices (Vehicular, Medical Devices, etc.)
      8. Incident response
      9. Principles – foundational knowledge units
      10. Operating Systems Security, foundation and advanced

11. Space Systems
12. Survey of modern cryptographic techniques and applications
13. Advanced Malware Analysis
14. Credential Compromise Reuse
15. Covert Communication Detection
16. Exploitation Detection Analysis

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 education programs in these areas to advance the state of the nation and to grow and expand the pool of qualified candidates for future employment. Proposals should include short-term objectives and expected long-term benefits of the collaborative partnerships with technical colleges, community colleges, or minority institutions.
    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. **Community Outreach:** Develop community outreach programs, such as partnerships with student and/or community organizations to encourage cyber and/or STEM related activities with minority students. Proposals may also address the continuing education and professional development of educators currently at the technical colleges, community colleges, and/or minority intuitions.

II. Examples of Activities:

- Laboratory equipment 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 cyber career fields and increased awareness of the potential security threats, vulnerabilities, and knowledge on improving the security posture for themselves and others around them.
- Faculty and student projects in cyber-related disciplines in order to develop a strong foundation for a cybersecurity program.
- Partnerships with DoD organizations and installations in the area of exercises and labs that improve their ability to train and educate their cyber workforce.

[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.*

- 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 in cybersecurity fields.
- Support to the National Guard Bureau to improve their ability to train and educate their cybersecurity workforce.
- Partnership with a minority institution to identify under-served and under-utilized potential students who need growth in their profession and/or identifying untapped professionals needing/wanting a mid-career change.

III. ANNEX II Technical Proposals:

In proposing support for capacity building activity, CAE technical proposals to ANNEX II must be clear and to the point and identify which of the two focus areas they are addressing. The proposal must also clearly address the following:

1. ***Sound & Reasonable Methodology*** - Institution demonstrates a sound method for achieving the stated goals. A timeline of activities is included.
2. ***Benefit to the CAE***: Institution demonstrates a clear benefit to the CAE.
3. ***Development Opportunities***: Institution demonstrates or outlines development opportunities for faculty and students of the CAE.
4. ***Benefit to the CAE Network and Cybersecurity Education***: Institution includes a plan to disseminate results of the proposed project to strengthen the cybersecurity education programs within and outside of the CAE network.
5. ***Student Interaction***: Institution describes how students will play an active role in the project.
6. ***Identified Partners***: Institutions provide contact (full name, email address, phone number, and mailing address) information for project partners or those who will benefit from the project.
7. ***DoD Partnerships***: Proposal should support key DoD priorities, including but not limited to: cloud computing, mobile technology, or other emerging needs as well as military organizations and support groups.
8. ***Outreach to Minority Institutions***: Proposals should include the development of meaningful, sustainable, results-oriented partnerships; or collaborations with minority institutions.
9. **Project Innovation**: Institution describes how this project is innovative.
10. **Costs**: Institution describes how the costs are reasonable in proportion to the scope of the proposal.

IV. 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 $300,000 or less in total ($150,000.00 per project).*** **Only one proposal per focus area may be submitted**.

V. 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 criteria identified in section *III. Annex II Technical Proposals* above as well as the following:

A. The CAE's current academic programs and proposed enhancements provide significant benefits to potential Cyber 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 CySP 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.

B. The costs of the proposal have been clearly articulated. Cost summations should be provided for:
   a. Total Funding Request for the Proposal;
   b. 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 must be realistic and reasonable.

C. Factors that will reduce the total evaluation score (if applicable). Those factors are:
   a. **Failure** to provide adequate administrative and/or academic support to current CySP students enrolled at the CAE institution.
      i. score reduction of 5 points
   b. **Failure** to properly invoice for previous CAE Cyber Grants within the allotted funding time.
      i. score reduction of 5 points for any grant older than 6 months with more than 50% funding remaining,
      ii. score reduction of 10 points for any funding over $50k returned one a grant)
   c. **Failure** to submit annual reports (CAE Annual Application reports as well as CAE Cyber Grant reports) as required.
      i. Score reduction of 5 points for each missing grant report
      ii. Score reduction of 5 points for each missing CAE Annual Report (For future grant solicitations, if the CAE has failed to submit the annual report two years in a row, the CAE will be ineligible to apply for the DoD CySP: scholarships and capacity building)

All Annex II proposals must be part of the larger university scholarship proposal and **postmarked on/before Thursday, 28 February 2019**.

Department of Defense
Cyber Scholarship Program (CySP)

DoD CySP Proposal Preparation Instructions
ATTACHMENT A

PROPOSAL FORMAT

All proposals must consist of a technical proposal and a cost proposal. Proposals must adequately describe the scholarship and capacity building objectives and approaches. All submissions will be evaluated by technical reviewers in accordance with the evaluation criteria during the selection process.

All provided forms must be used. **CAEs who submit a package not utilizing the designated forms, formats, or missing documents will be deemed incomplete and immediately disqualified and not considered for award.**

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 (Form 1)
        i. School Name
        ii. University Address
        iii. Name and Email Address of the Principal Investigator (PI), Project Director (PD), or Technical POC.
        iv. Pre Grant Negotiations Point of Contact(s): Name and Email Address
        v. Post Grant Issues (Invoices) Point of Contact(s): Name and Email Address
        vi. Provide a PDF copy of the most recent A-133 Summary of Auditor's Results. This should be one page. An example can be found here: https://www.iad.gov/NIETP/CAERequirements.cfm
    b. Proposal Summary: (continuation of Form 1)
        i. Funds Requested:

1. Basic Technical Proposal/ Recruitment Scholarship
2. Annex II/Capacity Building
3. Total

ii. Required Grant Start Date / Fall Semester Start Date

iii. **Mandatory Required Codes / Registrations (Provide a response for each)**

1. DUNS and Bradstreet - Data universal numbering system (DUNS) Number
2. Commercial and Government Entity (CAGE) Code:
3. Taxpayer Identification Number (TIN) or Employer Identification Number (EIN)

iv. Verify that the institution is registered and/or registration is current.

1. System for Award Management (SAM) https://www.acquisition.gov (printed copy of registration is required)
2. Acquisition Resource Center Registration (ARC) http://www.nsaarc.net/Index (printed copy of registration is required)

v. Signature of the Authorized University Official and the Date - Digital signatures are acceptable.

c. Complete form SF-424 – Application for Federal Assistance

d. Executive Summary (one page)

e. Sign and attach - Certifications 2019 (Attachment B)

f. Technical Proposal - Offerors shall mark their proposals to indicate the use of proprietary information and/or data. No more than 15 pages for each proposed. Be clear and concise.

i. Recruitment Program - Provide an overview of the program offered by the institution and how the students will be supported. The overview should include a description of the program advertisement and the student selection process.

ii. Retention Program – Provide an overview of the program offered by the institution and how the students will be supported. Current National Defense University partners should include a copy of your Memorandum of Understanding (MOU)

iii. Capacity Building Proposal – Additional information can be found in the ANNEX II section. Proposals should refrain from including extraneous information or lengthy discussions that do not pertain to the proposed project. Clear and concise and to the point

g. Cost Proposal

i. Cost and Student Endorsement (Attachment E)

ii. Offerors will submit a separate written cost proposal for: (no page limit on written cost proposal)

1. Recruitment/Basic Scholarship Program
2. Retention/Annex I Scholarship Program
3. Capacity Building Project(s)

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

h. CVs / Resumes are limited to 2 pages per faculty member and do not count towards the technical proposal page limits.

i. Recruitment / Basic Student Applications:

i. See student preparation instructions

ii. University must submit a student selection summary: Brief statement on each student and why they were recommended or not recommended.

iii. University must review the applications. The PI will initial the section to concur. One File per student, not one continuous file for all students. Saved in PDF format (NO PDF

Portfolios) with the following file name: ***LASTNAME_First Name_University***. PDF files should be editable and not locked. Handwritten applications will not be accepted. Student applications should not be saved as multiple PDFs (for example: one pdf for the application, another PDF for the resume, another for the transcripts…etc). If applications arrive not in the required format they will be deemed incomplete and not considered for a scholarship.

3. **Submission Format- 28 February 2019: Academic submission must arrive in both electronic and paper copy.** Any submission not arriving in both formats will be considered incomplete and not considered for award.
    a. ***Proposal order should follow 2A through 2H:***
        i. Proposal Cover Page and Summary – Form 1
        ii. SF424 – Form 2
        iii. Executive Summary
        iv. Attachment B - Certifications 2019
        v. A-133 Summary of Auditor's Results
        vi. Recruitment / Basic Scholarship – Technical Proposal
        vii. Recruitment / Basic Scholarship – Written Cost Proposal
        viii. Retention / Annex I Scholarship – Technical Proposal
        ix. Retention / Annex I Scholarship – Written Cost Proposal
        x. Capacity Building / Annex II – Technical Proposal
        xi. Capacity Building / Annex II – Written Cost Proposal
        xii. Attachment E – Cost and Student Rank Form 2019-2020 (Excel Format)
        xiii. SF-424A – Budget Information
        xiv. Written Student Endorsement Statement
        xv. Recruitment / Basic Student Applications
        xvi. CVs
    b. ***Submitting electronic copy:***
        i. **Preparing PDFs**:
            1. One (continuous) PDF of items 3.a.i through 3.a.xi, and 3.xiv. Saved as ***University Name_DoD CySP Submission Combined***.
            2. One PDF copy of 3.a.x and 3.a.xi. Saved as ***Unviersity Name_DoD CySP Capacity Building***
            3. Student applications – PDF (no PDF Portfolios, no separate PDF sheets). Saved as ***LASTNAME_First Name_University***
            4. Attachment E – Cost and Student Endorsement – **EXCEL FORMAT**
        ii. Proposals may be sent via email at: AskIASP@nsa.gov or by utilizing AMRDEC SAFE: https://safe.amrdec.army.mil/safe/guide.aspx Instructions are provided on this AMRDEC home page.
        iii. You may split the files up across multiple emails. A response to each email will be provided to ensure the current number of documents were received.
        iv. You may also send a google drive link, zipped file, or any other type of document sharing web interface.
    c. ***Submitting paper copy*:**
        i. DO NOT SEND: Thumb drives, CDs, DVDs, or any other type of removable media
        ii. Two (2) copies of 3.a.i through 3.a.ix and 3.iv.

iii. One (1) copy of 3.a.xii through 3.a.xiii
iv. Hard copies may be held together by paperclip or binder clip. Please do not staple documents or have them bound in a binder or clip folder.
v. Hard copy proposals should be sent to the addresses listed below.

DEADLINES

Institutionally approved, signed, completed proposals which include all items listed above and all student applications must be **postmarked or emailed on/before Thursday, 28 February 2019**. The entire proposal, containing all items listed above is to be mailed to:

DoD CySP National Security Agency
Attn: A233, NIETP, Suite 6804, Fanx 2
9800 Savage Road
Fort George G. Meade, MD 20755-6804

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

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 2018, 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.

Student Application Preparation Instructions

1. Students must use current forms
2. Form must be typed or electronically filled out. Unless prior arrangements have been made with the DoD CySP Program Office, hand-written applications (other than signatures/initials) will not be accepted.
3. Applications missing any required documents will automatically be disqualified
4. Students who are currently receiving funds from another scholarship program or who have a service obligation upon graduation are not eligible to apply for the DoD CySP.
5. Anticipated Final Graduation Date is for the degree program you are applying for scholarship support. Any applications that indicate a graduation date of January through September of the current year will not be eligible.
6. Transcripts: An official transcript is the institution's certified statement of the student's academic record. The official paper transcript is printed on security sensitive paper and contains the intuitions seal as well as a signature of the institution's registrar. An official electronic transcript is a PDF secured by a digital signature, which is displayed at the top of the transcript; sometimes they will include a blue ribbon.
    a. Paper application: Paper applications must include official transcripts. The institution's CySP point of contact or someone acting on his/her behalf may open transcripts. Applications arriving without official transcripts will be deemed incomplete.
    b. Soft copy application: Soft-copy (electronic) applications may contain a copy of the official transcript.
7. Students should not attach copies/pictures of social security cards, driver's license, passports, military identification, credit cards, degrees, certificates, and any other type of personally identifiable information. If any of these items are attached the application will not be accepted.
8. Letters of Recommendation should be an original version, not a copy, on official company/institution letterhead, include the contact information to confirm the letter is valid (full name, mailing address, phone number, email address) and must be signed by the author. Emailed letters will not be accepted.
9. Resumes should be limited to 2 pages and include but not limited to the following:
    a. Education: include degrees, institutions, location, date of graduation (or expected date of graduation); major/minor fields; GPA
    b. Experience: jobs, internships, and/or volunteer work. Include name of company, position, and dates employed. List at least three important tasks, accomplishments, or skills gained at each job. Also identify any clearance level held. It is important that you identify the number of hours per week you worked.
    c. Skills: include computer systems; programs which you are proficient. Include foreign languages. List any other skills, certifications, clearance levels you may hold.
10. Paper applications must be printed single sided on plain white 8 ½ x 11 paper.
11. Paper applications may be held together by a paper clip, rubber band, or binder clip. Do not staple or place in a binder.

12. Students are responsible for submitting a complete paper application to the CySP point of contact on campus.
13. Students may provide a PDF copy application to the CySP point of contact on campus.

Order of documents:

1. ***New Students:***
    a. DoD CySP New Student Application Form (10 pages)
    b. Official Transcripts
    c. Resume
    d. Separate List: Awards, Honors, and Distinctions (page 5 of the New Student Application)
    e. 2 Letters of Reference
    f. OF612 Supplemental Competency Statement (page 6 of the New Student Application)
2. ***Returning Students***:
    a. DoD CySP Returning Student Application Form (7 pages
    b. Official Transcripts
    c. Resume
    d. 1 Letter of Reference

Saving a PDF copy of the application:

Students should provide the IASP POC a PDF version of their application. Should a student not do so, the responsibility falls to the IASP POC. Student applications should be saved using the "reduced size PDF" when possible. There should be one file per student application. Do not save student applications as one continues PDF. PDF files should be use the following file name structure:

- ***NEW STUDENTS:***
    - **LAST NAME_First Name_University**
        - EXAMPLE: DOE_John_Worldwide University.pdf (CORRECT)
- ***RETURNING STUDENTS:***
    - LAST NAME_First Name_University_Returning

Adding additional words, numbers, or letters before or after the correct file name is not required and doing so slows down the process of compiling applications for the selecting DoD Agencies. Incorrect formats are as follows:

- Student Application_Doe_John_Worldwide.pdf (INCORRECT)
- Doejohnworldwideuniversity.pdf (INCORRECT)
- Worldwide University IASP Applications (INCORRECT)
- 11 – DOE_John_Worldwide University (INCORRECT)

PDF File size should not exceed 2.5 MB

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 Cyber Scholarship Program
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

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
	December 3, 2018