

# Department of Defense Cyber Scholarship Program

Sponsored by the  
DoD Chief Information Officer

## ***SOLICITATION FOR PROPOSALS***

From  
Universities designated under the  
National Centers of Academic Excellence in Cybersecurity (CAE-C)  
which includes  
*National Centers of Academic Excellence in Cyber Defense Education and  
National Centers of Academic Excellence – Research,*  
and  
*National Centers of Academic Excellence – Cyber Operations*  
(herein after referred to as CAE-Cs)

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

**Proposal Submission: 28 February 2020**

**SUBJECT TO AVAILABILITY OF FUNDS**

## CONTENTS

<b>II.</b>	<b>INTRODUCTION</b>
<b>III.</b>	<b>TERMINOLOGY</b>
	a. Cybersecurity
	b. Student Career Experience Program
<b>IV.</b>	<b>OVERVIEW OF PROGRAM SCOPE</b>
	a. Academic Year 2019-2020
	b. Capacity Building
	c. Proposal Formats
	d. Scholarship and Student Application Due Dates
	e. The DoD Role
	f. Future Opportunities
<b>V.</b>	<b>STUDENT OBLIGATIONS</b>
<b>VI.</b>	<b>CONDITIONS OF THE GRANT COMPETITION</b>
<b>VII.</b>	<b>CAE-C ROLE IN RECRUITING AND ASSESSING SCHOLARSHIP CANDIDATES</b>
	a. Announcing and Promoting the Program
	b. Managing the Application Review and Candidate Assessment Process
	c. Submitting Student Scholarship Applications and CAE-C Review and Endorsement
<b>VIII.</b>	<b>TECHNICAL PROPOSALS</b>
<b>IX.</b>	<b>COST PROPOSALS</b>
<b>X.</b>	<b>GRANT PROPOSAL EVALUATION CRITERIA AND SELECTION PROCESS</b>
<b>XI.</b>	<b>AWARDS</b>
<b>XII.</b>	<b>DEADLINE FOR SUBMISSION</b>
<b>XIII.</b>	<b>LATE SUBMISSIONS</b>
<b>XIV.</b>	<b>CONTACT INFORMATION</b>
<b>ANNEX II:</b> .....Institutional Capacity Building	
<b>ATTACHMENT A:</b> .....Proposal Preparation Instructions	
<b>ATTACHMENT B:</b> .....Certifications	
<b>ATTACHMENT C:</b> .....Scholarship and Vacancy Announcement	
<b>ATTACHMENT D:</b> .....Student Application	
<b>ATTACHMENT E:</b> .....Budget and Student Endorsement / Ranking Form (Excel Spreadsheet)	

## **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 under the National Centers of Academic Excellence in Cybersecurity (CAE-C) and known as National Centers of Academic Excellence in Cyber Defense Education or Research, and/or National Centers of Academic Excellence – Cyber Operations (hereinafter referred to as CAE-Cs) 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 2020- 2021. CAE-Cs may propose collaboration with other accredited institutions, and are encouraged to include accredited post-secondary minority institutions. CAE-Cs must be in good standing with the CAE-C Program Office and not be delinquent on any required documentation by the CAE-C Program Office. CAE-Cs 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-C 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-C Community College (pilot program) students who will be transitioning into a bachelor's degree program at a 4-year CAE-C
- 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. CAE-Cs 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-C'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 2020-2021.** The DoD estimates awarding scholarships (via grant awards) for a period of one year (beginning with the fall 2020 semester) to designated CAE-Cs, 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-C 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, CAE-Cs may also request funds for capacity building activities. Grant awards are contingent upon availability of funds.
- B. **Retention / Annex I Scholarships – Academic Year 2020-2021**
1. ***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](https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm). Community College CAE-Cs 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, CAE-Cs 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-C students to participate and gain additional understanding of cyber and cybersecurity as they relate to the extended community and DoD. Two main 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-C 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:** CAE-Cs 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 **Friday, February 28, 2020**. These dates are critical in order to ensure grant awards prior to August 1, 2020 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:** CAE-Cs 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-C. 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-C 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 pursuing 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. CAE-Cs 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-C's opinion, contributory to the student's academic progress; however, the development of students, not service to the CAE-C, 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 2020 and 2020.

#### **vi. CONDITIONS OF THE GRANT COMPETITION**

In order to be competitive in this grant solicitation, CAE-Cs 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-C’s assessment and recommendation of each proposed scholar’s capabilities and potential. CAE-Cs 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 CAE-Cs conduct the recruitment and assessment process.

#### **vii. CAE-C ROLE IN RECRUITING AND ASSESSING SCHOLARSHIP CANDIDATES**

If a CAE-C decides to participate in the recruitment/basic scholarship program, the following requirements apply:

- A. **Announcing and Promoting the Program:** The CAE-C 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-C 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-C 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:** CAE-Cs 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. CAE-Cs 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: CAE-Cs 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-C Endorsement. Please use Attachment E, Cost and Student Endorsement and Rank Form, for the following: CAE-Cs 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, CAE-Cs 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-C Review and Endorsement:** CAE-Cs 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 Cyber Scholarship 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-C**: Institution demonstrates a clear benefit to the CAE-C.
  3. **Development Opportunities**: Institution demonstrates or outlines development opportunities for faculty and students of the CAE-C.
  4. **Benefit to the CAE-C 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-C 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. **Support to DoD CySP**: Proposals should include the development of an annual DoD CySP Scholar Symposium.
  10. **Project Innovation**: Institution describes how this project is innovative.
  11. **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 CAE-Cs in the May 2020 timeframe. The grants will be awarded in the August 2020 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-C 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 CAE-Cs 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 CAE-Cs 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](mailto: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, unskewed 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 Friday, 28 February 2020**

#### **XVI. LATE SUBMISSIONS**

The CAE-C is responsible for electronically 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 emailed after the deadline of **28 February 2020** are “late,” and will **not** be considered for an award or scholarship.

Hard copy materials may arrive after the posted electronic copy due date.

#### **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: A29)  
Fort George G. Meade, MD 20755-6804  
410-854-6206  
e-mail: [AskCySP@nsa.gov](mailto:AskCySP@nsa.gov)