OMB CONTROL NUMBER: 0704-0486
OMB EXPIRATION DATE: XX/XX/XXXX

AGENCY DISCLOSURE NOTICE

The public reporting burden for this collection of information, 0704-0486, is estimated to average 44 per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

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 (NCAE-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 NCAE-Cs)

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

SUBJECT TO AVAILABILITY OF FUNDS

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 (NCAE-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 NCAE-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 2023- 2024. NCAE-Cs may propose collaboration with other accredited institutions, and are encouraged to include accredited post-secondary minority institutions. NCAE-Cs must be in good standing with the NCAE-C Program Office and not be delinquent on any required documentation by the NCAE-C Program Office.

Consistent with 10 U.S.C. 2200b, NCAE-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 DoD CySP. [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 2023-2024, students falling into one of the following categories may apply:

- Rising second-year NCAE-C Community College (pilot program) students who will be transitioning into a bachelor's degree program at a 4-year NCAE-C
- Juniors or Seniors pursuing a bachelor's degree (Sophomore's promoting to a Junior in Fall 2023 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. NCAE-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 Management or Administration
Business Process Analysis
Computer Crime Investigations Computer Engineering
Computer Programming
Computer Science
Computer Systems Analysis Cyber Operations
Cybersecurity
Cybersecurity Policy
Database Administration
Data Management
Data Science
Digital and Multimedia Forensics Electrical Engineering
Electronics Engineering
Information Security (Assurance)
Information Systems
Information Technology Acquisition
IT Program/Project Management
Mathematics
Network Management/Operations
Software Engineering
Systems Engineering

III. OVERVIEW OF PROGRAM SCOPE

The key elements of the DoD CySP, and the NCAE-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 2023-2024*** The DoD estimates awarding scholarships (via grant awards) for a period of one year (beginning with the Fall 2023 semester) to designated NCAE-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 NCAE-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, NCAE-Cs may also request funds for capacity building activities. Grant awards are contingent upon availability of funds.

(1) ***DoD Component / Agency Role***: NCAE-Cs are required to provide an assessment of each recruitment applicant which will be used by the DoD Component/Agency representatives reviewing student application. The actual selection of student scholars will be made by these DoD Component/Agency representatives. By selecting a student, a DoD Component/Agency agrees to provide clearance processing, a summer internship (if required), and full-time placement upon graduation. 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) ***Selected Recruitment Scholars Role***:

(a) 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 $22,000 for community college students (pilot program), $27,000 for undergraduate students and $32,000 for graduate (Master's/PhD) students. Awards will be made via a grant to the NCAE-Cs.

(b) 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.

(c) Students will be required to serve in internship positions, if timing permits, with the selecting DoD organization 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 organizations 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.

(d) 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.

(e) 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.

(f) Students will 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 principle investigator and the students in understanding these requirements before they apply.

(g) 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.

(h) 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.

(i) 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.

(j) Students will be required to agree to a code of conduct. A student handbook that includes the code of conduct rules will be provided to each selected student.

(k) Except for small achievement awards, not to exceed $6,000 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.

(3) ***NCAE-C Role***: Announcing and Promoting the Program: NCAE-Cs 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:

(a) Determine, communicate and publish to the relevant student populations web links, due dates, and Applicant Quick Start guide pertaining to the DoD CySP application cycle.

(b) Manage the Application Review and Candidate Assessment Process: NCAE-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 cyber work, and to provide a relative endorsement level for each eligible candidate. NCAE-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. All recommendation and KSA reviews will be done in the online DoD CySP Application tool.

(c) NCAE-C Endorsement. The NCAE-C will use the DoD CySP online application tool (https://www.avuedigitalservices.com/casting/aiportal/control/mainmenu?agency=DDW&portal=CYSP) to endorse all applying students. The endorsement for each applicant must include their 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, NCAE-Cs shall indicate only one of the following three levels of endorsement for each applicant:

1. Not Recommended
2. Recommended
3. Highly Recommended

(b) Submitting Student Scholarship Applications and NCAE-C Review and Endorsement: NCAE-Cs that propose to support the recruitment/basic scholarship program are required to review all applications in response to the announcement and to evaluate the applicants as described in detail above. Applications must be reviewed 28 February 2023 through the DoD CySP Online

Application Tool. https://www.avuedigitalservices.com/casting/aiportal/control/main-menu?agency=DDW&portal=CYSP The tool does not have a traditional "submit" button. As long as the NCAE-C has provided a ranking and recommendation statement by 28 February 2023, the student applicant will be considered for a scholarship. Additional instructions on requirements and submission formats are included in Attachment A, Proposal Preparation Instructions.

B. ***Retention / Annex I Scholarships – Academic Year 2023-2024***

(1) ***DoD Component / Agency Role*** – DoD Components and Agencies will nominate permanent DoD civilian and active duty military members according to the published DoD memo for one of following two programs:

a) ***Community College Scholarships***: 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 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.

b) ***Graduate Programs***: Active duty military members as well as permanent DoD civilian employees seeking to obtain a Master's or PhD at either the Naval Postgraduate School or the Air Force Institute of Technology may be nominated by their parent organization to be considered for a scholarship. Retention students do not apply directly to the NCAE-C.

(2) ***Selected Retention Scholars Role:*** 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 events. 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 2022. Retention Scholars will continue to receive their DoD/Military pay and will be required to perform a service obligation to their parent agency/component. Returning retention students will not be required to re-apply but must show progression in their degree program at the required GPA levels (3.0 for those pursing the community college option and a 3.2 for graduate programs (Air Force Institute of Technology, Naval Postgraduate School.)

(3) ***NCAE-C Role***:

a) ***Community College*****:** NCAE-Cs wishing to host retention scholars shall provide a written explanation of the course of study, if the program is in-resident or virtual/distance learning, how many students can be accommodated and how the NCAE-C will promote success with the retention students. Community College NCAE-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.

b) ***NCAE-C Partnership with National Defense University, College for Information and Cyberspace:*** NCAE-Cs wishing to partner with the NDU/CIC will be required to accept the DoD civilian employees or military officers into their graduate programs, who have successfully completed the CIC graduate level certificate program requirements. Requirements for addressing the NDU/CIC partnership option is described in Annex I, and should be responded to accordingly. 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). Please use Attachment E – Cost Form to identify costs per student, with a breakout of in-state/out-of-state (as applicable), MS and PhD/Doctorate (if both), and indicate the maximum number of partnership students you can accept during an academic year. The requirements for the student application nomination and review process described below and in the accompanying Student Application materials for the DoD CySP do not apply to current DoD/Federal civilian employees or military personnel whose applications for this program will be handled directly by the DoD as described in Annex I.

C. ***Capacity Building – Academic Year 2023-2024*** **This particular area is subject to the availability of funds**. In accordance with 10 U.S.C. 2200b, NCAE-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 NCAE-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. NCAE-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

IV. CONDITIONS OF THE GRANT COMPETITION

In order to be competitive in this grant solicitation, Academic institutions holding a current NCAE-C designation in good standing are eligible to participate in this grant offer. Performance on previous grant awards will be considered. To be considered in good standing, the institution must meet the following qualifications:

- Current on all reporting requirements, to include annual reports and reports required by previously assigned DoD CySP, GenCyber, or other NCAE-C grant opportunities;
- Timely submission of invoices for previous grant awards;
- Zero or minimal (under $1000) funding returned to the DoD on previous grants;
- Attendance at required NCAE-C meetings and events; and
- Minimum participation in NCAE-C activities, committees or working groups
- The NCAE-C will only accept one submission from the designated NCAE-C program(s) at the institution regardless of the number of designations (NCAE-CD, NCAE-R, NCAE-CO).

NCAE-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 NCAE-C's assessment and recommendation of each proposed scholar's capabilities and potential. NCAE-Cs will have four weeks to review all student applications (2 -28 February 2023) and are reminded to submit all required documentation by the due date 28 February 2023. Addressed below in paragraph VII are the specific requirements for advertising the scholarship among the candidate student populations, assessing student applications, and reporting on the process.

V. TECHNICAL PROPOSALS

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

VI. COST PROPOSALS

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

VII. GRANT PROPOSAL EVALUATION CRITERIA AND SELECTION PROCESS

A. The designated NCAE-C program on campus may nominate students outside the designated program of study as long as the degree program is cyber-related. The NCAE-C point of contact (lead for the NCAE-C designation) does not have to act as the principal investigator but they should be involved in some capacity.

B. *Recruitment/Basic Student Applications*:
   a. First-Time Applies or New Students will answer several questions within the online application tool to determine eligibility. Once eligibility is determined, the student will submit their application to the NCAE-C through the DoD CySP online application tool. NCAE-Cs will perform their review and provide the written recommendation within the same online application tool. Each DoD Component/Agency will have access to the tool to review applications based on the rules and policies that govern their agency.
   b. Returning DoD CySP Scholars who applied through the tool in 2022: These students will log-in to their original account and upload the required documents.
   c. Returning DoD CySP Scholars who were paper based in 2022: These students will continue to be paper based.

C. *Scholarship 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.
   a. Proposals will be evaluated against the following criteria:
      - The merits of the institution's proposed approach to designing and developing a robust DoD CySP 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 DoD 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.
   b. Proposals must include the following:
      - Identified Programs of Study for the students
      - Proposed plan of how to manage the students. Include any required meetings and events.
      - A copy of the institutions student code of conduct

D. *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 NCAE-C***: Institution demonstrates a clear benefit to the NCAE-C.
3. ***Development Opportunities***: Institution demonstrates or outlines development opportunities for faculty and students of the NCAE-C.
4. ***Benefit to the NCAE-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 NCAE-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.

VIII. PROPOSAL FORMATS

Attachment A Proposal Preparation Instructions - identifies proposals formats. At a minimum, the proposal must respond to either:

- Establishment/continuation of a DoD Cyber Scholarship Program (Recruitment/Basic),
- Establishment/continuation of a DoD Cyber Scholarship Program (Retention/Annex I).

One or both scholarship options must be submitted as part of the proposal in order to be eligible for any ANNEX II/Capacity Building opportunities.

IX. APPLICATION DUE DATES:

- New and returning 22-Cohort Recruitment Applications will have until 01 February 2023 to submit their application through the DoD CySP online tool. https://www.avuedigitalservices.com/casting/aiportal/control/mainmenu?agency=DDW&portal=CYSP
- Paper based returning DoD CySP Recruitment Scholars will have until 15 February 2022 to submit their paper applications to their DoD CySP On-Campus-Point of Contact. Returning Recruitment Scholars are not included in the online tool.
- NCAE-Cs are required complete all new recruitment applicant reviews in the online tool by 28 February 2023. Early review and submission of the student applications is acceptable. NCAE-Cs are required to submit all grant paperwork to include returning recruitment student paper applications via softcopy to AskCySP@nsa.gov by 28 February 2023. Following the soft copy submissions, NCAE-Cs are asked to mail two hard copy submissions. They may be mailed to the DoD CySP Program Office (mailing address listed below). The hard copies may arrive within a week or so of the due date as long as the school submitted the softcopy filed by 28 February 2023.
- See Attachment A – Proposal Preparation Instructions for more guidance.

X. AWARDS

Recruitment Scholarship notifications for students will be announced to the NCAE-Cs in the April 2023 timeframe. The grants will be awarded in the August 2023 timeframe. Awards will be made for one year only with a 15 month period of performance. Based on scholarship selections, the DoD may award a lower level of funding than what was proposed.

The DoD recognizes the considerable NCAE-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 NCAE-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 NCAE-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 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 Tuesday, 28 February 2023**

XVI. LATE SUBMISSIONS

The NCAE-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 2023** 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: A206)
Fort George G. Meade, MD 20755-6810
410-854-6206
e-mail: AskCySP@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 2023 and 2024

National Centers of Academic Excellence in Cybersecurity (NCAE-Cs) *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 DoD CySP requirements may be more stringent than general academic enrollment criteria for a particular college/university. No waivers will be granted.

Two-year Degree Scholarships (Community College/Institutions who offer 2-year cyber-related degrees): 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 or institution designated as a NCAE-Cs. A list of those institutions can be found at:
https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

a. NCAE-Cs 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 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.

National Defense University / College for Information and Cyberspace Partnership, focuses on DoD civilian employees and military officers who wish to pursue a full-time or part-time master's, PhD, or Doctorate in a cyber discipline. Applicants will be nominated to enter the program in either September 2023 or January 2024. Selected students will complete the first

part of their degree through NDU/CIC and then enter a partner NCAE-C university to complete the remaining degree requirements.

- Full-time students complete one of the NDU/CIC cyber certificates at a 14-week in-resident program at the Ft. McNair, Washington DC campus.
- Part-time NDU/CIC students may apply for the DoD CySP after they have completed 75% of the required courses for completion of the cyber-certificate program.
- Students must complete all NDU/CIC certificate requirements prior to continuing their study with one of the NCAE-C Partner Universities.

II. ANNEX I Technical Proposals

NCAE-Cs must be willing to consider acceptance of DoD-selected students who meet NCAE-C college/university entrance requirements.

NCAE-Cs 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:

NCAE-Cs 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 in ANNEX I, NCAE-Cs should estimate the per student scholarship costs for DoD students (e.g., tuition, books, and select academic fees). Unlike non-DoD (recruitment) students participating in the scholarship program, DoD retention students will not receive stipends. These scholarship costs should be identified separately from any other direct costs associated with the partnership proposed.

V. EVALUATION CRITERIA

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

A. The merits of the NCAE-C'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

NCAE-Cs *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 NCAE-C's basic proposal in response to the broader solicitation. **While scholarships will be funded prior to any capacity building, approximately $1,000,000, may be set aside for capacity building for academic year 2023-2024.**

NCAE-Cs may submit one proposal which provides a response to one or two focus areas identified below. The total proposal submission per NCAE-C may not exceed $300,000.00 ($150,000.00 for each project). Any proposals exceeding this limit will automatically 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, NCAE-Cs 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 NCAE-C 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.

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.
    d. **Advanced Cyber Enrichment Activities:** Building upon programs that provide cyber activities, provide cyber learning activities to students at an advanced level.

II. Examples of Activities:

- Laboratory equipment purchase and/or installation and lab exercises to be provided at non-NCAE-C 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.
- 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.

[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.*

III. ANNEX II Technical Proposals:

In proposing support for capacity building activity, NCAE-C 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 NCAE-C***: Institution demonstrates a clear benefit to the NCAE-C.
3. ***Development Opportunities***: Institution demonstrates or outlines development opportunities for faculty and students of the NCAE-C.
4. ***Benefit to the NCAE-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 NCAE-C 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. If contact information is missing, the proposal will be deemed incomplete.
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. NCAE-Cs are advised that the request ***shall be limited to $3000,000 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 NCAE-C's proposal package using the criteria identified in section *III. Annex II Technical Proposals* above as well as the following:

A. The designated NCAE-C program on campus must submit all proposals. The NCAE-C point of contact does not have to act as the principal investigator but they should be involved in some capacity.

B. The NCAE-C's current academic programs and proposed enhancements provide significant benefits to potential Cyber Scholarship students and support DoD mission needs. The NCAE-C 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.

C. The costs of the proposal have been clearly articulated. Cost summations should be provided for total funding request for the proposal.

D. 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 DoD CySP students enrolled at the NCAE-C institution.
        i. score reduction of 5 points
    b. **Failure** to properly invoice for previous NCAE-C, GenCyber, or DoD CySP 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 $10k returned on a grant within the past 3 years
    c. **Failure** to submit annual reports (NCAE-C Annual Application reports as well as NCAE-C, GenCyber, or DoD CySP Grant reports) as required.
        i. score reduction of 5 points for each missing grant report
        ii. score reduction of 5 points for each missing NCAE-C Annual Report (For future grant solicitations, if the NCAE-C has failed to submit the annual report two years in a row, the NCAE-C 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 Tuesday, 28 February 2023**.