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 2022-2023.**

NCAE-Cs may submit one proposal which provides a response to one, two, or all three of focus areas identified below. The total proposal submission per NCAE-C may not exceed $450,000.00 ($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, 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.

3. GenCyber Collaboration: In an effort to build partnerships, the DoD CySP is partnering with GenCyber to develop much needed tools for the Nation. DoD CySP participating institutions, who nominate students to the recruitment program and have successfully held either a teacher or student GenCyber camp within the last 3 years are eligible to propose a capacity building project for one of the topic areas below.
    a. **Development K-12 cybersecurity career awareness resources that reflect diversity.** Outcomes will be shared with other NCAE-Cs as well as GenCyber participants via CLARK/CARD and any additional sharing opportunities identified by the GenCyber Program Office.
    b. **Development of a pedagogical program on best practices for teaching K-12 cybersecurity.** Beyond teaching cybersecurity content, K-12 educators need experience with best practice methodologies in how to teach the cybersecurity content. Proposals in this category should come from experienced GenCyber Camp Hosts looking to continue work with teacher participants. Outcomes will be shared with other NCAE-Cs as well as GenCyber participants via CLARK/CARD and any additional sharing opportunities identified by the GenCyber Program Office.
    c. **Regional teacher learning community.** Develop a program or platform to provide year round professional development and engagement with K-12 cybersecurity teachers. Proposals in this category should come from experienced GenCyber Camp

[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.*

Hosts looking to continue work with teacher participants. Outcomes will be shared with other NCAE-Cs as well as GenCyber participants via CLARK/CARD and any additional sharing opportunities identified by the GenCyber Program Office.

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.

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.

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 $450,000 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:
   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.

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 $50k returned one 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, 15 February 2022**.