SOLICITATION

for

Universities, Colleges, Community Colleges, Public or Private Schools/Districts or Private (Not for Profit) Entities that Partner with an Aforementioned Institution

2022 GenCyber Grant Call for Proposals

CFDA: 12.903

CAMPS: Summer 2023

SECTION I – EXECUTIVE SUMMARY

GENERAL INFORMATION

This solicitation sets forth guidelines for areas of interest in cybersecurity education for eligible academic institutions for the GenCyber program.

The National Security Agency's, GenCyber Program, housed within the Center for Education, Innovation, and Outreach at the National Cryptologic School provides cybersecurity training programs for Middle and High School teachers and students in order to meet future national security challenges.

GENCYBER PROGRAM

GenCyber responds to a recognized need to develop cybersecurity awareness and teach sound cybersecurity fundamentals at the middle and high school levels. The program achieves this by providing grants to universities, public or private schools or school systems to conduct in-residence, commuter, virtual, or hybrid learning events for students and providing instruction, instructional materials, and effective teaching methods to middle and high school teachers.

MISSION AND VISION

> *Inspiring the next Generation of Cyber stars by working with academic and federal partners to ignite cybersecurity awareness and teach sound cybersecurity fundamentals that strengthen the K-12 cybersecurity ecosystem and the Nation's future workforce.*

The GenCyber program seeks to ignite and sustain cybersecurity interest in order to build a competent, diverse, and adaptable cybersecurity workforce pathway through alignment with the National Centers of Academic Excellence in Cybersecurity (NCAE-C). The GenCyber program will be a part of the solution to the Nation's shortfall of skilled cybersecurity professionals. The GenCyber program aligns with the NCAE-C program in order to provide awareness of college and career readiness pathway opportunities for students and educators. Program participants do not have to be designated NCAE-C institutions to apply to host a GenCyber program. The GenCyber program office works collaboratively with federal partners to ensure that the program continues to have a nation-wide impact on the middle and high school cybersecurity education ecosystem. To ensure a level playing field in developing cybersecurity career pathway opportunities, GenCyber camps and events are **FREE** to all student and teacher participants.

PROGRAM GOALS

The goals of the GenCyber program are to:

- Ignite, sustain, and increase awareness of cybersecurity content, and cybersecurity postsecondary and career opportunities for participants through year-round engagement.
- Increase student diversity in cybersecurity college and career readiness pathways at the K-12 level.
- Facilitate teacher readiness within teacher learning communities to learn, develop, and deliver cybersecurity content for the K-12 classroom in collaboration with other nationwide initiatives.

FUNDING

GenCyber is funded by the National Security Agency (NSA) and the National Science Foundation (NSF). Other federal partners may contribute funding on an annual basis.

SCHEDULE

Proposals are due no later than Friday, December 10, 2021 at 11:59pm EST. Grant awards are anticipated to be

announced by March 2022 with funding awarded in April 2022. Grant awards are effective two years from the date awarded (NSA Grant Office signature). Please consider this when writing your proposal. Institutions with at least one year of experience hosting a GenCyber program may elect to include an option year in the budget. The option year is not guaranteed.

PROPOSED TIMELINE

If funded, the following is an estimated timeline:

- *Summer 2022*: Proposal status notification (PoP: Summer 2022- Summer 2024)
- *Fall/Winter 2022*: Planning, marketing, recruiting
- *Winter/Spring 2023:* Pre-camp outreach activities
- *Summer 2023:* Summer camp experience
- *Fall/Winter 2023/Spring 2024*: Post camp outreach activities
- *Fall/Winter 2023* Option year notification (if applicable)
- *Summer 2024:* Finalize grant paperwork

ELIGIBILITY

This solicitation is open to any academic institution (college, university, community college, or K-12 school/school district) or a Not-for-Profit who agrees to partner with one of the institutions. Academic institutions may partner with other academic institutions on one proposal. Additional eligibility requirements are stated below:

- Applicants previously awarded a GenCyber grant must be current on all reporting requirements and may not be delinquent in submission of invoices for previous grant awards.
- Returning GenCyber grantees must comply with all other conditions of previous awards, to include attendance at mandatory meetings, filing of required reports, etc.
- Previous GenCyber grantee status does not guarantee a 2022 grant award.

National Center of Academic Excellence in Cybersecurity Applicants Only: The GenCyber Program Office will only accept submissions from the designated NCAE-C program(s) at the institution. Interested parties outside of the designated program path(s) must include written endorsement from the identified NCAE-C identified point of contact on campus. The NCAE-C POC can be involved either directly or indirectly with the proposal.

MANAGEMENT OF FOREIGN NATIONAL INVOLVEMENT ON GRANTS RESULTING FROM THIS SOLICITATION

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. It is the responsibility of the grantee to validate the citizenship of proposed individuals.

- Faculty (Principal Investigators (PI)/ Program Director (PD)/Co-PIs), Administration, Other Support Staff, all research assistants, student workers, anyone receiving a salary from the grant must be a US Citizen or permanent residents admitted to the U.S. for permanent residence.
- All instruction must occur in the United States (with the potential for U.S. territorial or tribal participation). GenCyber funds cannot be used to fund study programs abroad. The applying organization must not be organized, charted, or incorporated under the laws of any country other than the U.S. or its possessions or be controlled by an individual who is not a U.S. citizen. GenCyber funds may not be used to support a foreign-owned entity.
- All student and teacher program participants must reside in the United States and be enrolled in or teach at a United States school or home-schooled.

HUMAN SUBJECTS RESEARCH

The NSA GenCyber Program Office strongly discourages proposals that include the use of human subjects research. Should the offeror believe that the proposed project would absolutely need the use of human subjects the offeror must follow DoD and NSA rules and policies. The use of human subjects is required to be coordinated through the funding entity prior to the grantee performing any human subjects research activities funded by the grant. Once coordinated, human subject research, prior to occurring, shall adhere to DoDI 3216.02, NSA/CSS Policy 10-10, and any requirement imposed by the NSA/CSS Human Protections Administrator, including review by an applicable Institutional Review Board (IRB), the IRB's determination and, post-IRB determination, Human Research Protections Official review by the grantor.

PROPOSAL

Concise proposals addressing the offeror's plan are requested. Focus on the institution's commitment to the proposal, faculty and staff qualifications, and what the proposal offers to the subject of the project. It is not necessary to describe the state of cybersecurity, workforce or cybersecurity education in the United States. Proposals shall be submitted in accordance with guidance provided in Attachment A, Proposal Preparation Instructions.

AWARD TYPES AND FUNDING

Awards made as a result of this solicitation will be in the form of a Grant. Grant awards are effective two years from the date awarded (NSA Grant Office signature); there will be no extensions beyond the two-year timeframe. Please consider this when writing your proposal.

The 2022 GenCyber Program is offering the following distinct funding opportunities. GenCyber grant awards are anticipated to be $100,000- $175,000 each; dependent upon the proposed activity. The Program Office reserves the right to request a budget modification prior to final grant status notification.

Offerors may submit a proposal for each of the five (5) categories below. Offerors are cautioned to write clear and concise proposals that answers the requirements of the Proposed Program. Proposals that overlap multiple categories will automatically be disqualified. One proposal cannot be dependent on another category proposal. (Example: Your Student Camp Proposal cannot require activities from the Teacher Camp proposal.) Each proposal will be evaluated separately; therefore, one proposal must not be dependent upon another in any way.

REF #	Proposed Program	Additional Eligibility Requirements	Format	Description	Max Amt.	Option Available
22-S	Student	None	Face-to-Face; Virtual; Hybrid	30-hour summer camp with 24-30 hours of required pre/post camp outreach activities (54-60 hours total)	*$150,000*	***Y-1 year $150,000***
22-T	Teacher	None	Face-to-Face; Virtual; Hybrid	30-hour summer camp with 24-30 hours of required pre/post camp outreach activities (54-60 hours total)	*$150,000*	***Y-1 Year $150,000***

22-C	Combination	One year of successful GenCyber student camp experience AND 1 year successful GenCyber teacher camp experience	Face-to-Face; Hybrid	30-hour summer camp with 24-30 hours of required pre/post camp outreach activities (54-60 hours total) Additional 8-10 hours of teacher camp time is required 54-60 hours total for students; 62-70 for teachers)	*$175,000*	***Y-1 Year $150,000***
22-L	GenCyber Student Language Pilot Programs	One year of successful completion of a GenCyber student program; demonstration of expertise in foreign language education	Face-to-Face; hybrid	30-hour summer camp with 24-30 hours of required pre/post-camp outreach activities (54-60 hours total) GenCyber concepts and cybersecurity curriculum taught using immersion in one of five critical languages (Russian, Chinese, Arabic, Korean, and Persian), Spanish, or another language (with justification)	*$175,000*	*NO*
22-B	Capacity-Building	None	Virtual; Face-to-Face; Hybrid; or resource development	Proposals to allow for creative submissions for initiatives that will impact the GenCyber community.	*$100,000*	*NO*

SECTION II – PROPOSED PROGRAMS

2.1 CATEGORY DESCRIPTIONS

22-S. STUDENT PROGRAMS GenCyber student programs are those activities that ignite or sustain cybersecurity and cybersecurity career interest amongst middle or high school students.

- **Target Audience**. The intended audience of the student program is middle and high school participants. Programs focused on the K-5 level will be considered, but must focus on long-term engagement opportunities will be available to these young students. Further, the proposal must explain whether the program will recruit novice students or students with pre-existing experience in computer science and/or cybersecurity.
- **Budget**. The budget amount for a student program is no more than $150,000.
- **Contact hours**. The minimum number of contact hours with participants is 54 hours. The camp curriculum must include at least 30 instructional hours in cybersecurity education with an additional 24-30 hours of total pre-camp and post-camp engagement with the target audience. Proposals must include an overall program timeline of events, as well as a detailed schedule of activities and curriculum (the total number of instructional hours all events must be clear). Information regarding the format (hybrid, virtual, face-to-face) must be included.
- **Curriculum.** Each institution is responsible for developing a creative and age-appropriate curriculum that addresses the Cybersecurity Concepts, ethics, and cybersecurity careers while advancing the goals of the GenCyber program. Modules and pre-existing resources may be used with the considerations outlined in section 2.4.3.

- **K-12 Ecosystem**. Offerors must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and how the activity/program will further enhance the GenCyber community and the local environment. Institutions are encouraged to partner with other members of the local ecosystem to ensure continuity with or without GenCyber funding.
- **Diversity**. Proposals must specifically describe the targeted participants and how recruiting will engage those participants, and ensure that camp staff, curriculum, activities, events, and support mirror the best practices of working with the targeted audience. Proposals should include an explanation of how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants, etc. Proposals should reflect local geographical diversity and demographics in the proposed curriculum. Vague references to diversity or reaching diversity goals are not sufficient.
- **Option**. Offerors who have one or more years of experience hosting a GenCyber program may include a proposal for one additional option year, not to exceed $150,000 in funding. Offerors may propose an advanced camp with current base-year attendees or repeat the base-year camp structure with new attendees. Option year details, including curriculum, number of camps, participants, etc., should be described and uploaded in the "Other" section. Option awards are not guaranteed. All awards (Base or Option) are subject to availability of funds. The GenCyber Program Office will use performance outcomes from the base year to determine if an option may be awarded.

22-T. TEACHER PROGRAMS. GenCyber Teacher Programs are those activities that offer teachers professional development to implement cybersecurity in multiple disciplines or to give teachers the tools to develop stand-alone computer science/cybersecurity courses for the local school.

- **Target Audience**. The intended audience of the teacher program is middle and high school teacher participants. Further, the proposal must explain whether the program will work with computer science/cybersecurity teachers or teachers from a wide range of disciplines. Either target audience is appropriate, but the proposed structure and curriculum must align with the target audience. In order to facilitate the success of this program, all teacher participants must have a letter of support from his/her school administrator. This letter must be requested during the recruitment phase of planning.
- **Budget**. The budget amount for a teacher program is no more than $150,000. Institutions are permitted to budget for one teacher participant to attend the GenCyber 2022 Fall Meeting (in addition to the Program Director and Lead Instructor). The institution will be expected to provide the Program Office a name as well as the rationale of how the individual was chosen at registration.
- **Contact hours**. The minimum number of contact hours with participants is 54 hours. The camp curriculum must include at least 30 instructional hours in cybersecurity education that includes teaching teacher participants' cybersecurity content knowledge and HOW to teach cybersecurity content in a classroom setting. An additional 24-30 hours of total pre-camp and post-camp engagement with the target audience is also required. Proposals must include an overall program timeline of events, as well as a detailed schedule of activities and curriculum (the total number of instructional hours all events must be clear). Information regarding the format (hybrid, virtual, face-to-face) must be included.
- **Curriculum.** Each institution is responsible for developing a creative and age-appropriate curriculum that addresses the Cybersecurity Concepts, ethics, and cybersecurity careers while advancing the goals of the GenCyber program. Modules and pre-existing resources may be used with the considerations outlined in section 2.4.3.
- **Lesson Plans.** Teacher participants must leave camp with a minimum of two usable lesson plans. Time must be allotted for lesson plan development and feedback on both the development and the presentation of these plans.
- **K-12 ecosystem and GenCyber Community.** Offerors must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and how the activity/program will further enhance the GenCyber community and the local environment. Institutions are encouraged to work with teacher participants to build a local/regional Teacher Learning Community (TLC). To further strengthen these

relationships with and among teacher participants, institutions can (and are encouraged to) invite teachers to local cybersecurity events (conferences, campus events, etc.) that occur outside the realm of the GenCyber program. However, please note that these events **do not** count towards the 24-30 hours of pre-camp and post-camp outreach requirements. *Institutions are encouraged to partner with other members of the local ecosystem to ensure continuity with or without GenCyber funding.*

- **Diversity.** Proposals must specifically describe the targeted participants and how recruiting will engage those participants, and ensure that camp staff, curriculum, activities, events, and support mirror the best practices of working with the targeted audience. Proposals should include an explanation of how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants, etc. Proposals should reflect local geographical diversity and demographics in the proposed curriculum. Vague references to diversity or reaching diversity goals are not sufficient.
- **Option**. Offerors who have one or more years of experience hosting a GenCyber program may include a proposal for one additional option year, not to exceed $150,000 in funding. Offerors may propose an advanced camp with current base-year attendees or repeat the base-year camp structure with new attendees. Option year details, including curriculum, number of camps, participants, etc., should be described and uploaded in the "Other" section. Option awards are not guaranteed. All awards (Base or Option) are subject to availability of funds. The GenCyber Program Office will use performance outcomes from the base year to determine if an option may be awarded.

22-C. Combination Programs. GenCyber Combination Programs are those activities that seek to offer teachers professional development to implement cybersecurity in multiple disciplines or to give teachers the tools to develop stand-alone computer science/cybersecurity courses for the local school while also offering student participants the activities that ignite or sustain cybersecurity and cybersecurity career interest amongst that age group. In order to compete for this proposal, the proposal must provide evidence of the institution's track record of success working with both students and teachers. Competing in this category requires 1 year of GenCyber student camp experience and 1 year of GenCyber teacher camp experience.

- **Target Audience.** The intended audience of the combination program is middle and high school participants. Further, the proposal must explain whether the program will work with computer science/cybersecurity teachers or teachers from a wide range of disciplines. Either target audience is appropriate, but the proposed structure and curriculum must align with the target audience. Due to the difficulties of hosting a successful combination program, the proposal must be very detailed and concise as to who is learning what content, how, when, and why.
- **Budget.** The budget amount for a teacher program is no more than $175,000. Institutions are permitted to budget for one teacher participant to attend the GenCyber 2022 Fall Meeting (in addition to the Program Director and Lead Instructor). The institution will be expected to provide the Program Office a name as well as the rationale of how the individual was chosen at registration.
- **Contact hours.** The minimum number of contact hours with student participants is 54 hours. Teacher participants must complete an additional 8-10 hours of instruction in order to have sufficient time to develop and receive feedback on lesson plans, making their minimum number of contact hours 62. The camp curriculum must include at least 30 instructional hours in cybersecurity education that includes teaching teacher participants' cybersecurity content knowledge and HOW to teach cybersecurity content in a classroom setting. An additional 24-30 hours of total pre-camp and post-camp engagement with the target audience is also required. Proposals must include an overall program timeline of events, as well as a detailed schedule of activities and curriculum (the total number of instructional hours all events must be clear). Information regarding the format (hybrid or face-to-face) must be included. A combination camp cannot be hosted in a purely virtual setting unless local safety issues require this format.
- **Curriculum.** Each institution is responsible for developing a creative and age-appropriate curriculum that addresses the Cybersecurity Concepts, ethics, and cybersecurity careers while advancing the goals of the

GenCyber program. Modules and pre-existing resources may be used with the considerations outlined in section 2.4.3.

- **Lesson Plans.** Teacher participants must leave camp with a minimum of two usable lesson plans. Time must be allotted for lesson plan development and feedback on both the development and the presentation of these plans.
- **K-12 ecosystem and GenCyber Community.** Offerors must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and how the activity/program will further enhance the GenCyber community and the local environment. Institutions are encouraged to work with teacher participants to build a local/regional Teacher Learning Community (TLC). To further strengthen these relationships with and among teacher participants, institutions can (and are encouraged to) invite teachers to local cybersecurity events (conferences, campus events, etc.) that occur outside the realm of the GenCyber program. However, please note that these events do not count towards the 24-30 hours of pre-camp and post-camp outreach requirements. Institutions are encouraged to partner with other members of the local ecosystem to ensure continuity with or without GenCyber funding.
- **Diversity.** Proposals must specifically describe the targeted participants and how recruiting will engage those participants, and ensure that camp staff, curriculum, activities, events, and support mirror the best practices of working with the targeted audience. Proposals should include an explanation of how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants, etc. Proposals should reflect local geographical diversity and demographics in the proposed curriculum. Vague references to diversity or reaching diversity goals are not sufficient.
- **Option**. Offerors who have one or more years of experience hosting a GenCyber program may include a proposal for one an additional option year, not to exceed $150,000 in funding. Offerors may propose an advanced camp with current base-year attendees or repeat the base-year camp structure with new attendees. Option year details, including curriculum, number of camps, participants, etc., should be described and uploaded in the "Other" section. Option awards are not guaranteed. All awards (Base or Option) are subject to availability of funds. The GenCyber Program Office will use performance outcomes from the base year to determine if an option may be awarded.

22-L. GenCyber Student Language Pilot Program. GenCyber language programs are those student activities that ignite or sustain cybersecurity and cybersecurity career interest amongst middle or high school students through immersion in one of the critical languages. Submission of a Language Program proposal requires one year of successful completion of a GenCyber program as well as a demonstration of expertise in foreign language education.

- **Target Audience.** The intended audience of the student program is middle and high school participants that speak/study/or are fluent in one of the five critical-need languages (Arabic, Chinese, Korean, Persian, and Russian), Spanish, or another specific language with strong justification. Further, the proposal must explain whether the program will recruit novice students or students with pre-existing experience in computer science and/or cybersecurity. Details on incoming language proficiency of participants should also be included.
- **Budget.** The budget amount for a student program is no more than $175,000.
- **Contact hours.** The minimum number of contact hours with participants is 54 hours. The camp curriculum must include at least 30 instructional hours in cybersecurity education with an additional 24-30 hours of total pre-camp and post-camp engagement with the target audience. Proposals must include an overall program timeline of events, as well as a detailed schedule of activities and curriculum (the total number of instructional hours all events must be clear). Information regarding the format (hybrid, virtual, face-to-face) must be included.
- **Curriculum.** Each institution is responsible for developing a creative and age-appropriate curriculum that addresses the Cybersecurity Concepts, ethics, and cybersecurity careers while advancing the goals of the

GenCyber program. Modules and pre-existing resources in the target language may be used with the considerations outlined in section 2.4.3.

- **K-12 ecosystem.** Offerors must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and how the activity/program will further enhance the GenCyber community and the local environment. Institutions are encouraged to partner with other members of the local ecosystem to ensure continuity with or without GenCyber funding. Proposers should demonstrate best practices in immersion education.
- **Diversity**. Proposals must specifically describe the targeted participants and how recruiting will engage those participants, and ensure that camp staff, curriculum, activities, events, and support mirror the best practices of working with the targeted audience. Proposals should include an explanation of how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants, etc. Vague references to diversity or reaching diversity goals are not sufficient.
- **Language immersion ecosystem:** Curriculum must be taught in one of the five critical-need languages, Spanish, or another justified language. Proposal must include percentage of time for target language immersion (e.g. 75%).

22-B. Capacity Building Activities. GenCyber Program Office welcomes unique and impactful GenCyber capacity-building projects. Capacity-building projects are those that work to ignite or sustain engagement beyond the scope of a structured camp environment. Because all funded proposals have an outreach requirement, these activities must go beyond required outreach events.

- **Budget.** The anticipated amount of funding under this category of GenCyber grants is no more than $100,000.
- **Contact hours.** While there is no minimum-contact hour requirement, a timeline addressing development, implementation/action, etc. must be included as applicable to the proposed project/activity.
- **Curriculum/types of activities.** The following activities are encouraged by the Program Office; however, this list is not an extensive list – creative and innovative ideas are welcome!
  - Activities or resources that allow participants to continue to engage in cybersecurity exploration or career activities beyond the scope of a structured program
  - Activities or projects that benefit a region or the entire GenCyber program
  - Activities or resources that focus on increasing diversity in cybersecurity college and career readiness
  - Activities or resources that further expand upon other GenCyber or National Centers of Academic Excellence in Cybersecurity (NCAE-C) funded initiatives (i.e., CAE RING project)
  - Activities or resources that build or sustain teacher learning communities in a local or wide region
  - Activities that seek to engage with other stakeholders in the K12 ecosystem (administration, counselors, career coaches, etc.).
  - Activities that seek or continue to engage underrepresented populations in the K12 ecosystem

SECTION III - GRANT SUBMISSION INFORMATION

3.1 APPLICATION REQUIREMENTS

To be eligible for GenCyber grant funding under this solicitation, all proposal submissions must meet the following threshold criteria. **Please note that there are additional requirements depending upon the specific proposal you would like to submit. You can see those in Section 2 above.**

- **BRANDING:** All activities funded under this grant must be branded as GenCyber activities and include GenCyber in the camp title. Institutions must acknowledge this requirement and are encouraged to use GenCyber branded items at their camp. Items purchased or provided by other partners should not be branded as GenCyber.
- **STAFF EXPERTISE:** In order to be successful, camp staff should have the following expertise:
  - **K-12 Expert**. Use of a K-12 pedagogical expert (an individual with K12 classroom experience) in the curriculum development and camp delivery is a requirement. Camp staff selection must align with the needs and abilities of the target audience.
  - **Cybersecurity Knowledge.** Instructors should have a solid understanding of cybersecurity concepts and practices.
  - **Teacher Training**. For GenCyber teacher and combination programs, camp staff must have previous experience training teachers**.**
- **COST:** Camps are to be free to all participants**.**
- **SAFETY:** All programs funded under this grant must include a safety plan to ensure that all participants (students and teachers alike) can learn in a safe, secure environment for the duration of the program.
- **CURRICULUM:** Proposals must adhere to age-appropriate standards and performance-based cybersecurity learning programs in a safe environment for students in middle and/or high school, as appropriate.
  - **THE GENCYBER CYBERSECURITY CONCEPTS** are fundamental to understanding and practicing effective cybersecurity. They also represent the foundation upon which cybersecurity mechanisms are reliably built and cybersecurity policies can be reliably implemented. **Each GenCyber program must use the GenCyber Cybersecurity Concepts as the foundation of their camp.** The proposal must discuss how the various lessons (e.g., cryptography, Python programming, drone hacking, basic digital forensics, cybercrime, or network defense and attack) are unified by the Concepts. Proposals can incorporate the First Principles, if desired, but the foundation should be based on the concepts. The GenCyber Concepts are below. Full definitions of these and the First Principles are available in Appendix C.
    - Defense in Depth
    - Integrity
    - Think Like an Adversary
    - Confidentiality
    - Availability
    - Keep it Simple
  - **ETHICS:** Ethics is a critical part of cybersecurity. In order to ensure this understanding (and future practice) of GenCyber participants, it is imperative that cybersecurity ethics are also foundational to the curriculum.
  - **CYBERSECURITY CAREERS:** An awareness and understanding of the potential opportunities available in the field of cybersecurity is a goal of the GenCyber program. Curriculum must include at least one unit and/or activity that introduces program participants to the many opportunities available in cybersecurity. Examples include guest speaker panels, use of the NICE workforce framework, the use of interactive resources in which participants explore potential careers, etc.
  - **PRE-EXISTING CURRICULUM:** GenCyber does not provide curriculum; however, it is permissible to use pre-existing modules and resources. When using these pre-existing curricula, time must be spent to ensure that the use of curriculum is presented in a way that is age-appropriate and unique to this GenCyber program. When using this curricula, the GenCyber program office expects to clearly see that less time is spent on curriculum development than would otherwise be should an institution choose to create completely unique curriculum.
- **FORMAT:** Camp formats can be face-to-face, virtual, or hybrid. Combination programs must have some Face-to-Face interaction and therefore cannot be solely virtual. All GenCyber camps (Student, Teacher, Combination, and Language) are expected to run a minimum of five days to include at least 30 intensive instructional hours. Programs also must offer at least 24-30 hours of pre-camp and post-camp outreach.

- Instructional hours are defined as those blocks of time in which participants are actively engaged in learning (lecture, guest speakers, labs, hands-on activities, field trips, etc.).
- If conducting a virtual experience, participants must know how to receive support when participating in instructional activities. Those institutions wishing to offer virtual experiences must describe how program goals will be accomplished in a virtual setting (i.e. how will the institution ensure that interest in cybersecurity increases as a result of the virtual experience). Virtual experiences should include structure and detailed schedules to result in maximum participation of the target audience.
- Breaks and lunch breaks that do not include educational activities are not included in the 30-hour minimum. It is recommended that participants receive multiple breaks throughout the day and at least 30 minutes of uninterrupted lunch.
- Programs less than five contact days are insufficient to adequately meet the goals of the program. Proposals that do not meet or exceed the minimal number of hours will not be considered for funding.

- **SCHEDULE CONSIDERATIONS:** When scheduling GenCyber events, consideration must be given to dates that could potentially be affected by religious observations (i.e., Ramadan), local school/community events, other campus-hosted camps, or holidays (i.e., Independence Day).
- **AUDIENCE:** Proposing institutions must be detailed in describing the target audience and diversity goals and relate how the recruitment/retainment strategies, camp curriculum, and camp staff will ensure that the targeted participants gain skills and interest in cybersecurity. Institutions should include activities that increase awareness of postsecondary opportunities and careers in cybersecurity.
- **COMMUNICATION:** Camps must participate in all surveys and requests for information from the Program Office and contract support.

GRANT PROPOSAL SUBMISSION

See Attachment A – Proposal Preparation Instructions

SELECTION PROCESS

Proposals will be evaluated by a panel of Department of Defense and Federal Agency cyber professionals drawn from, but not limited to, the National Security Agency, Department of Homeland Security, Federal Bureau of Investigation, National Institute of Standards, U.S. Cyber Command, as well as Military Departments, and the Office of the DoD Chief Information Officer.

EVALUATION CRITERIA

The Government anticipates multiple awards as a result of this Grant Solicitation, however, the Government reserves the right to select for award all, some or none of the proposals received, if it is determined to be in the best interest of the Government. The actual number of grants awarded will depend on the number of complete and acceptable proposals, cost of individual awards, availability of funds and geographic locations.

The evaluation is a complete assessment of the offerors proposal. Decisions to fund selected proposals are based on the selection criteria identified below and the ability of funds. As a result of funding constraints, not all proposals deemed selectable may be funded. Awards resulting from the Grant Solicitation will be made by the Government, considering cost and non-cost factors. Where there are no significant differences in the evaluation of non-cost factors among proposals determined selectable, and such proposals are found to be equally important in support of critical need foreign languages education, then funds availability alone will be the determining criterion for award. **Prior GenCyber Grantee status does not assure a 2022 grant award.**

The GenCyber Program Office shall use price analysis techniques to determine price reasonableness. These methods of evaluation may include information/input from sources such as, but not limited to, other grant programs and personnel. The GenCyber team reserves the right to require the submission of any data (e.g., data other than cost and pricing) necessary to validate the reasonableness of an offer.
Proposals will be evaluated against the following criteria:

- **Eligibility** – The proposal, the offeror and all coalition members meet the eligibility requirements listed in paragraph 1.3.
- **Sound & Reasonable Methodology** - Institution demonstrates a sound method for achieving the stated goals. A timeline of activities is included as appropriate.
- **Quality and Experience** – Proposals must clearly state the qualifications of the offeror and the proposed team members to fulfill the objectives of the solicitation, and certifies each participant's professional commitments allow time to perform on the grant. The Program Office reserves the right to consider past performance and demonstrated competence in final award decisions. Coalition proposals clearly specify the role of each participant, and the lead institution provides evidence of grant management expertise.
- **Deliverable** – Proposal clearly specifies plans for required deliverables, and those plans meet the required deliverables of the solicitation. The proposal acknowledges the deliverable will be provided to the NCAE-C Program Office and will be made available to the NCAE-C Community as appropriate.
- **Solicitation Objectives** – The proposal includes detailed description of how the proposal meets the objectives of the solicitation.
- **Identified Partners** - Institutions provide contact information for project partners and clearly delineates each partner's responsibilities.
- **Cost** – Institution describes how the costs are reasonable in proportion to the scope of the proposal. In cases where multiple proposals meet requirements and are evaluated to be equal in quality of proposal and ability to fulfill objectives, the Program Office will evaluate the cost of the proposal against the proposed methods, deliverables, and associated costs and will select the best return on investment for cost.
- **Project Innovation** – In cases where the solicitation specifically asks for innovative solutions, the proposal describes how this project demonstrates innovation.
- **Clarity** – The solicitation clearly accounts for all solicitation requirements.

AWARDS
Refer to chart found on pages 4-5.

REPORTING/DISSEMINATION
Awardees will be required to deliver reports based on the following schedule:

Report #	Report Name	Report Due Date
1	Planning/Pre-Camp Outreach	***1 April 2023*** (or 30 days following pre-camp outreach completion, whichever comes first)
2	Camp Report	30 Days Post Camp
3	Final Technical Report / Three (3) Lesson Plans (with post-camp outreach)	01 September 2024 (or 30 days following post-camp outreach completion, whichever comes first)
4	Final Federal Financial Report (SF-425)	The recipient must submit, no later than 120 calendar days after the end date of the period of performance, all financial, performance, and other reports as

		required by the terms and conditions of the Federal award

In addition to what was identified in your proposal, you agree to possibly provide any outcomes to the GenCyber Program Office, DoD (Agencies and Components), US Government Agencies/Components, the National Centers of Academic Excellence in Cybersecurity Program. You also agree to share outcomes with other academic institutions to include NCAE-Cs and the CAE Community when appropriate.

- Projects may be included in several national repositories that the DoD may identify at a later date (example: CLARK, CARD, etc). Please keep in mind that curriculum, labs and other education resources may be available to all US educational institutions. Items may also be published to the NCAE-Cs via the CAE Community Website and/or CAE Application Database as appropriate. Grant language 32 CRF 32.36 and 2 CFR 200.315 gives the Federal Government the right to "(1) Obtain, reproduce, publish or otherwise use the data first produced under an award; and (2) Authorize others to receive, reproduce, publish or otherwise use such data for Federal purposes." - **As a result, it is the expectation that grantees produce curricula materials in a manner that would not prevent the Government from exercising its rights listed herein. It is the responsibility of the curriculum developer to ensure that all provided materials are either original material or have been appropriately sourced to permit the Government to exercise its contractual rights**
- Regarding 508 Compliance: All delivered materials, documentation and information technology will meet the NSA Information Communications Technology Accessibility Standards, derived from Section 508 of the Rehabilitation Act (29 USC 795d) and Web Content Accessibility Guidelines 2.0 AA requirements.

OTHER ITEMS

- 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."
- Grants and Cooperative Agreements - As defined in the DOD Grants and Agreements Regulations, DoD 3210.6-R, a grant is "A legal instrument which, consistent with 31 U.S.C. 6304, is used to enter into a relationship:
    - Of which the principal purpose is to transfer a thing of value to the recipient to carry out a public purpose of support or stimulation authorized by a law of the United States, rather than to acquire property or services of the Department of Defense' direct benefit or use.
    - In which substantial involvement is not expected between the Department
    - The Government is not obligated to make any award as a result of this solicitation.

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

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/

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.

CERTIFICATE OF LIABILITY INSURANCE

Applicants ***must*** provide a certificate of liability insurance to document that student safety, liability, and insurance issues are addressed. This certificate ***must*** be submitted with the proposal.

DEADLINE FOR SUBMISSION

See the proposal preparation instructions for details on the submission of proposals. Institutionally approved, signed, completed proposals must be submitted electronically through the GenCyber Proposal System on/before Friday, 10 December 2021. In addition, two hard copies (unbound, single-side printed page) of ALL required documents (including Certificate of Liability and all others listed in PPI) must be mailed to the program office with a postmark of the 10 December 2021 due date.

LATE SUBMISSIONS

The institution is responsible for electronically submitting the proposal to the GenCyber Grants Program Office at the National Security Agency by the date and time specified.

INCOMPLETE PROPOSALS

Proposals submitted in the wrong format, using wrong forms, or missing items will be deemed incomplete and will not be considered for an award.

CONTACT INFORMATION

The central points of contact for information regarding this solicitation is:

GenCyber Grants Program Office
National Security Agency
9800 Savage Road
SUITE 6810
Fort George G. Meade, MD 20755-6810
410-854-8994
GenCyber@nsa.gov

GenCyber Cybersecurity Concepts

Defense in Depth – A comprehensive strategy of including multiple layers of security within a system so that if one layer fails, another layer of security is already in place to stop the attack/unauthorized access.

- A castle is secured by a moat, a drawbridge and guards at the gate.
- Your home computer is secured by locks on the door, an alarm system, and a firewall.
- Company data is secured by a firewall, passwords, and encryption.

Confidentiality – The property that information is not disclosed to individuals, devices, or processes unless they have been authorized to access the information.

- Student grades can only be accessed by specific individuals within the organization, such as authorized teachers and the principal.
- At a hospital, medical information about a patient is protected and only provided to authorized personnel.
- Salary information is typically only available to authorized personnel within a company, such as the supervisor and human resources.

Integrity – The property that information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

- Student grades are accurate and have not been modified by an unauthorized user.
- A website is the entity it claims to be.
- A computer system is virus-free and uncompromised.

Availability – The property that information or information systems are accessible and usable upon demand**.**

- A student's grades can be viewed by the student and principal and modified by the teacher.
- A website for a store is allowing orders to be placed and viewed.
- A banking system is appropriately accessible by both customers and banking employees.
- A Denial-of-Service attack can result in a system being unavailable and inaccessible.

Think Like an Adversary – The strategy of putting yourself inside the mindset of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly.

- In order to best protect a student's data, it is useful to think of potential adversaries and their motivations, such as a student wishing harm on another, a student seeking to modify his own data, and consider possible strategies – breaking physically into an office, breaching a network to obtain unauthorized access, etc. and build your security strategy accordingly.
- Discussions on ethics of a cybersecurity professional must correlate with any activity in which adversarial thinking is being modeled.

Keep It Simple – The strategy of designing information and security systems to be configured and operated as simply as possible; all systems perform best when they have simple designs rather than complex ones.

- A complex alarm system can have many points of failure, including the hardware and the software.
- A complex computer system has many points of access and may be difficult to secure. A simple solution is often the best strategy.

GenCyber Cybersecurity First Principles

Data Hiding – The principle of keeping information inaccessible except within the process itself.

- The programming concept of making data private rather than public.
- A student's grades cannot be viewed by anyone except the teacher, parent, and the student.

Abstraction – The principle that the interface of a hardware or software component must be independent of its implementation.

- In Object Orientated Programming, objects are used to represent complex data structures.

Resource Encapsulation – The process of separating an entity (system, object or hardware) to include and isolate its own data.

- In object-oriented programming, encapsulation is the inclusion within a program object of all the resources needed for the object to function – basically, the methods and the data.

Modularity – The process of separating functionality into independent pieces to ensure each piece performs a separate function and keeps its own data.

- Using functions or methods in programming is an example of modularity.
- Modularity within the system architecture enforces security by keeping operating system functions separate and unique.
- Modular design means focus in on building small carefully crafted components that are used throughout the application.

Layering – The process of providing multiple layers of protection or controls between critical data and attackers; layered security can be considered one step of defense-in-depth strategy.

- A security solution to protect your home computer may include – an antivirus, a firewall, parental controls, and privacy controls.
- In computer programming, layering is the organization of programming into separate functional components that interact in some sequential and hierarchical way, with each layer usually having an interface only to the layer above it and the layer below it.

Least Privilege – The principle of allowing entities (people, processes, devices) only the capabilities necessary to accomplish their assigned duties and functions.

- The term need-to-know is a restrictive information policy often used in the military that means you share information only with the individuals that need-to-know, only the facts they need-to-know at the time they need to know them and nothing more.

Domain Separation – Implies that data, processes, and systems must logically define their area of control (domain).

- A ruler has control of his own region only.
- Teachers can only modify grades for students in their classes.

Process Isolation – Ensuring that programs or operating systems run completely separate from other programs or operating systems for the purpose of controlling access to system resources memory.

- Process isolation is frequently used in web browsers to separate multiple tabs and to protect the core browser itself must a process fail.

Simplicity - the quality of designing programs, systems, and processes to be free of complexity, easier to test, easier to operate, easier to protect.

- A simpler system design will reduce the attack surface area and make it easier to secure the system.

Minimization – keeping all design and functionality aspects to a minimum, reducing needless size and complexity.

- Data minimization is the practice of limiting the collection of information to only that which is directly relevant and necessary to accomplish a task. This policy will also reduce exposure in the event of a breach.
- System minimization implies the practice of only running software, applications, or services necessary to perform the required function. This strategy not only increases security, but also can improve performance and save storage space.