(U) Solicitation

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

2021 GenCyber Grant Call for Proposals

Estimated Period of Performance Dates:

August 2021-August 2023

(Camps: Summer 2022)

Grant Authority: CFDA 12.903 GenCyber Grants Program

2021 GenCyber CFP Table of Contents

2021 GenCyber Grant Call for Proposals (CFP)

SECTION I: GenCyber Executive Summary

1.1 GenCyber Program Summary

The National Security Agency's National Cryptologic School provides cybersecurity training programs for Elementary, Middle, and High School (K-12) teachers and students in order to meet future national security challenges.

GenCyber responds to a recognized need to develop cybersecurity awareness and teach sound cybersecurity fundamentals at the K-12 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 (ex. summer camps held during May-September timeframe; capacity-building opportunities in local schools); and providing instruction, instructional materials, and effective teaching methods to elementary, middle, and high school teachers. If a not-for-profit organization/institution would like to participate in the GenCyber program, they may partner with a college/university/community college or a public or private school and that academic institution will have to apply. Grants will only be issued to an academic institution.

1.2 GenCyber Vision & Mission:

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 at the K-12 level in order to build a competent, diverse, and adaptable cybersecurity workforce pipeline 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. Ensuring that enough young people are inspired to utilize their talents in cybersecurity is critical to the future of our country's national and economic security as we become even more reliant on cyber-based technology in every aspect of our daily lives. The program also increases cybersecurity hygiene practices for all participants therefore increasing the security posture of the nation. The GenCyber program aligns with the NCAE-C program in order to provide awareness of college and career pathway opportunities for K12 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 K12 cybersecurity education ecosystem. To ensure a level playing field in

developing cybersecurity career pathway opportunities, GenCyber camps and events are offered **FREE** to all student and teacher participants.

1.3 GenCyber Program Goals:

The goals of the GenCyber program include

- Igniting, sustaining, and increasing awareness of K12 cybersecurity content and cybersecurity postsecondary and career opportunities for participants through year-round engagement.
- Increasing student diversity in cybersecurity college and career readiness pathways at the K-12 level.
- Facilitating teacher readiness within a teacher learning community to learn, develop, and deliver cybersecurity content for the K-12 classroom in collaboration with other nationwide initiatives.

1.4 Funding Organization

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

1.5 Grant Award Information

1.5.1 GenCyber grant awards are anticipated to be $100,000- $200,000 each; dependent upon the proposed activity (as described in Section II). Programs with unique program circumstances can submit a request to exceed the maximum amount of award, but there must be a clear and concise justification included. The Program Office reserves the right to request a budget modification prior to final grant status notification.

1.5.2 Due to the increased interest in the GenCyber program, grant award competition has increased. Accordingly, previous GenCyber grantee status does not guarantee a 2021 grant award.

1.5.3 Proposals are due 60 days after date of solicitation release. Grant awards are anticipated to be announced by June 2021 with funding awarded in August 2021. Grant awards are effective for two years from the date awarded.

1.5.4 Please be aware that if awarded a grant, there will be no period of performance extensions beyond the two-year timeframe.

1.5.5 Due to the 2-year Period of Performance of the grant~~;~~ the following reporting requirements are necessary if awarded a Student, Teacher, Combination, or "GenCyber Goes Virtual" Teacher camp grant. All reports must be submitted to the Program Office via email.

a) Report 1: Planning/Pre-Camp Outreach Report (due NLT 1 Feb 2022)—General overview of planning, the finalized version of the summer camp or activity, and plans for pre-camp engagement activity.

b) Report 2: Camp report—report summarizes the final happenings of the camp and pre-camp outreach. This report is due NLT 30 days of the last date of the camp. Camp must occur in the summer months of 2022.

c) Report 3: Final technical report and 3 lesson plans—An overall summary detailing the planning, pre-camp outreach, camp event, and post-camp outreach. This plan is due NLT 30 days after the end of the PoP of the grant. This is the report that ONR will require acceptance of prior to closing out the institution's grant. Three lesson plans must be submitted along with the final technical report.

d) Reports 1 & 3 are required for funded GenCyber Capacity-building projects.

1.6 Requirements for ALL GenCyber Programs

1.6.1 Proposals must adhere to age-appropriate standards and performance-based cybersecurity learning programs in a safe environment for students in elementary, middle, and/or high school, as appropriate.

1.6.2 Utilization 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.

1.6.3 All student and teacher program participants must reside in the United States and be enrolled in a United States school or home-schooled. Camps are to be offered free to all participants.

1.6.4 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. For more information see, Section IV, 4.1.11.

1.6.5 All GenCyber camps (Student, Teacher, Combination) are expected to run a minimum of one week to include at least 30 intensive instructional hours.

a) Programs also must offer at least 16-20 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.).

b) 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.

c) 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.

d) Programs less than five 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.

1.6.6 GenCyber camps are not intended to be conducted solely as preparation for cyber competitions or cybersecurity certifications.

1.6.7 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).

1.6.8 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.

a) Institutions should include activities that increase awareness of postsecondary opportunities and careers in cybersecurity.

1.6.9 All grants will have a 2-year Period of Performance (PoP) allowing for sufficient and ample time to plan, prepare, and conduct meaningful and engaging activities.

a) The camp experience must occur during the summer months of 2022.

b) A detailed timeline of events is now required for each proposal.

c) Institutions should the ability to host virtual offerings, if the need arises.

1.6.10 Camp formats can be face-to-face, virtual, or a hybrid approach.

a) Combination programs must have some aspect of face-face interaction and therefore cannot be solely virtual.

b) The proposal must describe why the proposed format was chosen and describe how GenCyber program goals will be accomplished using the proposed format.

1.6.11 Camps must participate in all surveys and requests for information from the Program Office and contract support.

1.6.12 The total number of accepted proposals is dependent upon funding. The Program Office will consider all factors such as adherence to program goals, diversity, past performance (if applicable), geographical location, etc. in the final funding decisions.

SECTION II: 2021 GenCyber Funding Opportunities

2.1 GenCyber Programs Offered

The 2021 GenCyber Program is offering the following distinct funding opportunities:

- GenCyber Student Program
- GenCyber Teacher Program
- GenCyber Combination Program
- "GenCyber Goes Virtual" Teacher Camps (Pilot)
- GenCyber Capacity-Building Activities

The GenCyber program has shifted from being a distinctly summer camp program to becoming a program that focuses on year-round outreach with a targeted audience.

Competing in each funding category requires a distinct and separate proposal. Institutions may not compete for multiple funding opportunities on one submitted proposal. Each proposal will be evaluated separately; therefore, one proposal must not be dependent upon another in any way. Institutions must carefully read all aspects of the CFP to ensure the proposal is eligible to be reviewed.

GenCyber 2021 Call for Proposals

Proposed GenCyber Project	Format	Description	Max Grant Amount ($)
GenCyber Student Programs	Face-Face; Virtual; Hybrid	Traditional summer camp with at least 30 hours of instruction; student-centered; required pre/post camp outreach activities (16-20 hours); total 46-50 hours	$150,000
GenCyber Teacher Programs	Face-Face; Virtual; Hybrid	Traditional summer camp with at least 30 hours of instruction; teacher-centered; required pre/post camp outreach (16-20 hours); total 46-50 hours	$150,000
GenCyber Combination Programs	Face-Face; Hybrid	Traditional summer camp with at least 30 hours of instruction (+8-10 for teachers only); required pre/post camp outreach (16-20 hours); student & teacher centered; requires 1 year of GenCyber student camp experience + 1 year of GenCyber teacher camp experience; cannot occur in pure virtual fashion (unless no other option exists); total 46-50 hours students and 54-60 teachers	$175,000
"GenCyber Goes Virtual" Teacher Camps	Virtual	Virtual camps with at least 30 hrs. of instruction for specific teacher populations in three specific geographical areas (Baltimore City/Native American) + one other region; pre/post-camp outreach activities required (16-20 hrs.), total 46-50 hrs.; institution agrees to support teachers through entire PoP of the grant, requires 1+ yrs. GenCyber teacher camp experience or validation of high levels of experience in teacher development (in cybersecurity)	$200,000
GenCyber Capacity-Building Activities	Virtual; Face-Face; Hybrid	Proposals to allow for creative submissions for initiatives that will impact the GenCyber community. Activities or ideas that allow for continued participant engagement in cybersecurity content or careers outside of a structured environment are encouraged. Ideas that seek to engage underrepresented groups are of particular interest. Projects with a regional or nation-wide impact are encouraged.	$100,000

2.2 GenCyber Student Programs

2.2.1 GenCyber Student Programs are those activities that ignite or sustain cybersecurity and cybersecurity career interest amongst middle or high school students.

a) The target audience must be middle or high school students.

- The proposal must explain whether the program will recruit novice students or students with pre-existing experience in computer science and/or cybersecurity.
- Programs aimed at grades K-5 will be considered but must focus on how local long-term engagement opportunities will be available to these young students.

b) The minimum number of contact hours with students is 46 hours.

- The proposal must include 16-20 hours of total pre-camp and post-camp engagement with the target audience.
- The camp curriculum must include at least 30 instructional hours in cybersecurity education.

c) All activities funded under this grant must be branded as GenCyber activities.

- Institutions who receive funding are encouraged to use GenCyber branded items at their camp (and these items should be included in the budget).
- The proposal must acknowledge the requirement for GenCyber branding in the proposal narrative.

2.2.2 Institutions wishing to propose ideas under this section of the CFP must be sure to describe in detail:

a) The ways in which the proposed activity or activities will further enhance the GenCyber community and the local K12 environment;

b) an overall program timeline of events;

c) the proposed format of the events;

d) a detailed schedule of the activities and curriculum (the total number of instructional hours of all events must be clear);

e) the targeted audience and predicted impact of the events;

f) an explanation of how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants;

g) proposers must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and the participants who will

participate. (Example: a program targeting novice learners must have a different format and curriculum than a program that proposes to serve students who have taken a computer science course).

2.2.3 Vague references to diversity or reaching diversity goals are not sufficient. 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.

2.2.4 Proposals that rely on an established curriculum or pre-existing resources must note the resources in the proposal.

a) The GenCyber program does not supply curriculum. Use of a pre-existing curriculum must be reflected in reduced time budgeted by instructional staff in the budget submission forms.

b) Those institutions developing new curriculum must budget for the time spent in unique curriculum development.

2.2.5 The budget amount for GenCyber grants under this category is no more than $150,000.

2.2.6 All student participants ***must*** reside in the United States and attend a school or be homeschooled in the United States.

2.2.7 If funded, the expected timeline for this category is described below.

a) Summer 2021: Proposal status notification (PoP summer 2021-summer 2023)

b) Fall-Winter 2021/Spring 2022: Planning, marketing, recruiting, pre-camp outreach event

c) Summer 2022-Summer camp experience

d) Fall/2022-Spring 2023-Post camp outreach event

e) Spring-Summer 2023—Finalized grant paperwork

2.3 GenCyber Teacher Programs

2.3.1 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.

a) The target audience must be middle or high school teachers.

- 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.
- Programs aimed at grades K-5 will be considered but must focus on how elementary school teachers will be supported by local environmental factors to impact students.

b) The minimum number of contact hours with teacher participants is 46 hours.

- The proposal must include 16-20 hours of pre-camp and post-camp engagement with the target audience.
- The camp curriculum must include at least 30 instructional hours in cybersecurity education that includes teaching teacher participants cybersecurity content knowledge and teaching teacher participants HOW to teach cybersecurity content in a classroom setting.
- Institutions are encouraged to work with teacher participants to build a local/regional Teacher Learning Community (TLC).
- Institutions are encouraged to invite teachers to local cybersecurity events (conferences, campus events, etc.) that occur outside the realm of the GenCyber program. These local events **do not** count towards the 16-20 hours of pre-camp and post-camp outreach requirements but would strengthen relationships with local teachers.

c) All activities funded under this grant must be branded as GenCyber activities, and proposals must address how this will be accomplished.

d) 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.

2.3.2 Institutions wishing to propose ideas under this section of the CFP must be sure to describe in detail:

a) the ways in which the proposed activity or activities will further enhance the GenCyber community and the local K12 environment;

b) an overall program timeline of events;

c) the proposed format of the events;

d) a detailed schedule of the activities and curriculum (the total number of instructional hours of all events must be clear);

e) an explanation of how, why, and when participants will learn cybersecurity content with the understanding that teacher participants must learn cybersecurity content AND how to teach cybersecurity content;

f) the targeted audience and predicted impact of the events;

g) an explanation of the reasons how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants;

h) time allotted for lesson plan development and feedback on lesson plan development;

i) proposers must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and the participants who will participate. (Example: a program targeting multidisciplinary teachers must have a different format and curriculum than a program that proposes to work with teachers who have developed a stand-alone cybersecurity course).

2.3.3 Proposals that rely on an established curriculum or pre-existing resources must note the resources in the proposal.

a) The GenCyber program does not supply curriculum. The use of a pre-existing curriculum must be reflected in the time budgeted by instructional staff in the budget submission forms.

b) Those institutions developing new curriculum must budget for the time spent in curriculum development.

2.3.4 The anticipated amount for GenCyber grants under this category is no more than $150,000.

2.3.5 All teacher participants ***must*** reside in the United States and be a teacher or plan to become a teacher at a school in the United States.

2.3.6 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.

2.3.7 If funded, the expected timeline for this category is described below.

a) Summer 2021: Proposal status notification (PoP summer 2021-summer 2023)

b) Fall-Winter 2021/Spring 2022: Planning, recruiting, pre-camp outreach event

c) Summer 2022 -Summer camp experience

d) Fall/Winter 2022-Spring 2023-Post camp outreach event

e) Spring-Summer 2023—Finalized grant paperwork

2.4 GenCyber Combination Programs

2.4.1 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.

a) The target audience must be middle or high school students and teachers.

- The proposal must explain whether the program will recruit novice students or students with pre-existing experience in computer science and/or cybersecurity.
- 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.
- Programs must focus on participants enrolled in or teachers of grades 6-12.

b) The minimum total number of contact hours with student participants is 46. The minimum number of contact hours with teacher participants is 54.

- The proposal must include 16-20 hours of total pre-camp and post-camp engagement with all participants.
- The camp curriculum must include at least 30 intensive instructional hours in cybersecurity education for all participants.
- Teacher participants must complete an additional 8-10 hours of instruction. This requirement fulfills the need for teachers to have sufficient time to develop and receive feedback on lesson plans.

c) Institutions are encouraged to work with teacher participants to build a local/regional Teacher Learning Community (TLC). Institutions are encouraged to invite participants to local cybersecurity events.

d) All activities funded under this grant must be branded as GenCyber activities, and proposals must address how this will be accomplished.

e) All teacher participants must have a letter of support from his/her school administrator. This letter must be submitted during the

recruiting phase.

2.4.2 Institutions wishing to propose ideas under this section of the CFP must be sure to describe in detail:

a) the ways in which the proposed activity or activities will further enhance the GenCyber community and the local K12 environment;

b) the required overall program timeline of events;

c) the proposed format of the events and who will participate;

d) a detailed schedule of the activities and curriculum and how individual participant's needs are served by the proposed curriculum (the total number of instructional hours of all events must be clear);

e) an explanation of how, why, and when teacher participants will learn cybersecurity content with the understanding that teacher participants must learn cybersecurity content AND how to teach cybersecurity content;

f) allotted time for teacher participants to develop and receive feedback on lesson plans;

g) the targeted audience and predicted impact of the events;

h) an explanation of the reasons how/why activities have been adapted to consider cultural, economic, and societal differences amongst participants;

2.4.3 Proposers must ensure that the proposed program is developed with knowledge of the local K12 ecosystem and the participants who will participate. (Example: a program targeting multidisciplinary teachers must have a different format and curriculum than a program that proposes to work with teachers who have developed a standalone cybersecurity course).

2.4.4 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 + 1 year of GenCyber teacher camp experience.

2.4.5 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. A combination camp cannot be hosted in a purely virtual setting unless local safety issues require this format.

2.4.6 The anticipated amount for GenCyber grants under this category is no more than $175,000.

2.4.7 All student and teacher participants ***must*** reside in the United States and be student or a teacher or plan to become a teacher at a school in the United States.

2.4.8 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 and rationale for how the individuals were chosen at registration.

2.4.9 If funded, the expected timeline for this category is described below.

a) Summer 2021: Proposal status notification (PoP summer 2021-summer 2023)

b) Fall-Winter 2021/Spring 2022: Planning, recruiting, pre-camp outreach event (institution can hosted students and teachers in combined event or host separate events for each participant group)

c) Summer 2022 -Summer camp experience

d) Fall/Winter 2022-Spring 2023-Post camp outreach event

e) Spring-Summer 2023—Finalized grant paperwork

2.5 "GenCyber Goes Virtual" Teacher Camps (Pilot)

2.5.1 This funded project represents a GenCyber Pilot Project; therefore, the awardee may be asked to submit a comprehensive and unique final report. Current and ongoing communication with the Program Office will be requested.

2.5.2 Institutions may form a coalition or partnership with other institutions or organizations to conduct this pilot. Roles and responsibilities of each participating organization must be specified in the proposal. In this case, one grant will be provided to the lead organization with sub-awards as appropriate.

a) Institution(s) must have at least one 1 year of GenCyber teacher camp experience or validation of high levels of experience in teacher development (in cybersecurity).

2.5.3 The GenCyber Program Office will fund one or more institution(s) to host a series of THREE "GenCyber Goes Virtual" Teacher Camps, with separate camps for each identified population.

2.5.4 The proposal must include an overall timeline of the activities to occur.

2.5.5 The minimum number of contact hours with teachers is 50.

a) The proposal must include 20-24 hours of total pre-camp and post-camp engagement with the target audience.

b) The camp curriculum must include at least 30 instructional hours in cybersecurity education.

c) Institutions are encouraged to work with teacher participants to build a Teacher Learning Community (TLC).

2.5.6 Camps must fulfill all the requirements of a GenCyber teacher program as listed in this CFP above (Section 2.3).

2.5.7 The preferred populations of these camps are a.) teachers in Baltimore City, b.) teachers on a Native American reservation who have an interest or will in the future be teaching cybersecurity, computer science, Career and Technical Education (CTE), and/or business, and c.) teachers from one other geographical location that represents a high-need population.

a) The proposal must validate teacher participants who do not teach in these content areas.

b) Emphasis must be placed on teachers who teach grades 9-12.

c) The funded institution must communicate all three geographical locations to the funding office NLT February 2022.

2.5.8 Teacher participants from each area must have a letter of support from his/her administrator.

2.5.9 Proposals under this section of the CFP must demonstrate the institution's ability to offer a virtual learning environment that focuses on the GenCyber Cybersecurity Concepts, online safety, cyber ethics, and career awareness. Curriculum may include Principles in addition to the Concepts.

2.5.10 The proposal must demonstrate the institution's ability to recognize and work with diverse groups while recognizing cultural differences.

2.5.11 Competing under this section of the CFP requires at least one year of hosting teacher camps in the GenCyber program.

2.5.12 All activities must be branded GenCyber activities, and proposals must address how this will be accomplished.

2.5.13 The anticipated amount of this project is no more than $200,000.

2.5.14 All teacher participants ***must*** reside in the United States (including tribal lands and US territories) and be a teacher or plan to become a teacher at a school in the United States, on tribal lands and/or US territories.

2.5.15 Institutions are permitted to budget for one teacher participant from each of the geographical areas (3 K-12 teachers total) to attend the GenCyber 2022 Fall Meeting (in addition to the Program Director and Lead Instructor). The institution will be expected to communicate with provide the Program Office a name and rationale for how the individuals were chosen at registration.

2.5.16 If funded, the expected timeline for this category is described below. More detail will be provided by the Program Office upon grant notification.

a) Summer 2021: Proposal status notification (PoP summer 2021-summer 2023)

b) Fall-Winter 2021/Spring 2022: Planning, recruiting, pre-camp outreach event (institution can hosted students and teachers in combined event or host separate events for each participant group). Three specific target teacher populations due to Program Office.

c) Summer 2022-Summer camp experiences

d) Fall~~/~~2022-Spring 2023-Post camp outreach event;

e) Spring-Summer 2023—Finalized grant paperwork

2.6 GenCyber Capacity-Building Activities

2.6.1 The 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. Due to the fact that all funded proposals now have a required pre/post camp outreach, these activities must go beyond required outreach events.

2.6.2 Activities or resources that allow participants to continue to engage in cybersecurity exploration or career activities beyond the scope of a structured program are encouraged. **Activities or projects that benefit a region or the entire GenCyber program are encouraged.**

2.6.3 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) are encouraged.

2.6.4 Activities that seek to engage with other stakeholders in the K12 ecosystem are encouraged (administration, counselors, career coaches, etc.).

2.6.5 Activities that seek or continue to engage underrepresented populations are encouraged.

2.6.6 A timeline addressing development, implementation/action, etc. must be included as applicable to the proposed project/activity.

2.6.7 All participants must reside in the United States and be a staff member or plan to become a staff member at a school in the United States or be a student enrolled in a US school or be homeschooled.

2.6.8 The anticipated amount of funding under this category of GenCyber grants is no more than $100,000.

2.6.9 Proposals in this category **must not** rely on the successful funding of any other GenCyber proposals.

SECTION III: GenCyber Program Information

3.1 GenCyber Meetings

3.1.1 The GenCyber program holds two meetings each year for the Program Directors and Lead Instructors. The meetings occur to communicate program-wide information, allow for networking and sharing of information, communicate best practices in K12 cybersecurity education, communicate federal partner projects in K12 education, and highlight different programs in order to strengthen the GenCyber community.

3.1.2 The Spring meeting is typically held in late April/early May and the Fall meeting is typically held in mid/late September. Meeting dates and formats will be communicated as early as possible. Although face to face meetings are preferred, the Program Office may elect to host a virtual meeting.

3.1.3 The Program Director and Lead Instructor (or their proxies as approved by the GenCyber team) are **required** to attend all GenCyber meetings. Attendance is reserved to two attendees per awarded grant. Any institution awarded a teacher program may elect to budget for one teacher participant to attend the 2022 Fall meeting only. This is not a requirement but optional for each individual institution.

3.1.4 Proposal budgets must include travel costs for both the Program Director and Lead Instructor (and teacher participant, if applicable) from each camp to attend these meetings. For the purpose of budget estimation worksheets, assume travel to Baltimore for THREE 2-day meetings.

3.2 GenCyber Curriculum

3.2.1 The GenCyber Program Office does not provide curriculum. Each institution is responsible for developing a creative and age-appropriate curriculum that addresses the GenCyber First Principles and/or Cybersecurity Concepts while advancing the goals of the GenCyber program. The Principles and Concepts are included below.

3.2.2 GenCyber will provide a lesson plan template to be used for your summer camp activities and/or exercises. It is required that lesson plans (a minimum of 3) be delivered with final reports at the end of your program. These lessons plans will be shared publicly, once an appropriate venue is developed, to further the goal of improving teaching methods for delivering cybersecurity content in K-12 curricula. Strengthening the Nation's cybersecurity posture, particularly through cybersecurity education at all levels in order to foster the knowledge and skills of individuals who may

ultimately join the U.S. Government, is an important Federal purpose. The lesson plans will be made available for others to reproduce, publish, and use them in furtherance of this Federal purpose. Lesson plans and associated deliverables must meet 508 compliance for accessibility. Further details are included later in the CFP.

3.3 GenCyber Cybersecurity First Principles & Concepts

3.3.1 The GenCyber Cybersecurity Principles and 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 select one of the following frameworks: a) GenCyber Cybersecurity First Principles or b) GenCyber Cybersecurity Concepts on which to base its curriculum. Regardless of the selected framework, **ALL** First Principles or Concepts within that framework must be incorporated into the curriculum at least at an introductory level. Furthermore, 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 chosen curriculum framework.

3.3.2 Definitions for the following GenCyber Cybersecurity First Principles and Concepts can be found in Appendix C.

GenCyber Cybersecurity First Principles

Data Hiding	Least Privilege
Abstraction	Domain Separation
Resource Encapsulation	Simplicity
Modularity	Process Isolation
Layering	Minimization

GenCyber Cybersecurity Concepts

Defense in Depth	Confidentiality
Integrity	Availability
Think Like an Adversary	Keep it Simple

3.4 Site Visits

Pedagogy, creativity, and innovation are high priorities of the GenCyber Program Office. All first-year institutions will have a site visit to observe one day of the camp. The Program Office will make selections for visits to experienced camps, virtual and hybrid camps, and Capacity-Building Activities. The Program Office and its contracted support reserves the right to visit any GenCyber event being hosted. The purpose of the Site Visit is to offer real time feedback and support to program participants.

3.5 Surveys

3.5.1 Surveys are distributed to Program Directors for participants to fill out on the first and last day of camp. Surveys may also be required for pre/post camp events. The surveys are specific to the target participants of the activity. The purpose of the student survey is to assess interest in cybersecurity and report on GenCyber's goal of increasing interest and career interest in cybersecurity. Interest is a critical motivational variable and has been found to influence: 1) what people pay attention to, when, and for how long, 2) levels of learning and achievement, 3) effort, and 4) goals. The student survey measures various aspects of interest and interest development from each camp for the GenCyber program as a whole. Demographic data may also be collected in order to assess whether the GenCyber program is successful in increasing student diversity in cybersecurity pathways. Responses from the student surveys also provide suggestions for improving each camp to promote interest development.

3.5.2 The purpose of the teacher survey is to assess teaching/coaching readiness in order to report on GenCyber's goal of facilitating teacher readiness to deliver cybersecurity content for the K12 classroom. The teacher survey looks at each GenCyber camp as a Professional Learning Community and provides an assessment of teacher readiness to teach/coach cybersecurity. Teaching/Coaching Readiness is calculated and reported as an aggregate score for all camp participants who indicated their reason for attending the camp was to transition what they learned into profession practice. Responses from the teacher surveys also provide suggestions for improving each camp to promote teaching/coaching readiness.

3.5.3 The surveys used for a combination camp will be targeted to each specific audience and will contain the information listed in the above two paragraphs. Completion of these surveys is an important aspect of program reflection and growth.

3.5.4 Surveys may be given to program participants at GenCyber Capacity-Building Activities, but this will be communicated by the Program Office on a case-by-case basis.

3.6 Camp Metrics

Performance metrics will be used to make future funding decisions. Submission of all required grant deliverables, site visit evaluations, performance snapshot reports, survey results, and other camp management metric gatherings will be used by the Program Office for future program enhancements and decisions.

SECTION IV 2021 GenCyber Grant Proposal Eligibility Requirements

4.1 Eligibility for All GenCyber Funded Proposals

To be eligible for GenCyber grant funding under this solicitation, all proposal submissions must meet the following threshold criteria:

4.1.1 The institution applying must be a university, public or private school or school system. Non-profit organizations must partner with one of the above applying institutions to be eligible.

4.1.2 All program/camp titles or activities must include the name GenCyber. For example, University GenCyber Teacher Camp or Community College GenCyber Academy.

4.1.3 A valid DUNS (Data Universal Number System) number ***must*** be included in proposal submissions. If your institution does not have one, apply for one ***immediately*** to allow for receipt in time to submit your proposal before the deadline. You can apply for a DUNS number at the following website: http://fedgov.dnb.com/webform/index.jsp.

4.1.4 A FICE (Federal Interagency Committee on Education) number must be included in college/university proposals, must your institution have one of these numbers. Institutions other than colleges and universities are not required to include a FICE #.

4.1.5 A current CAGE (Commercial and Government Entity) code ***must*** be included in proposal submissions. If your institution does not have one, apply for one ***immediately*** to allow for receipt in time to submit your proposal before the deadline. You can apply for a CAGE code at: http://www.sam.gov

4.1.6 Applicants must be registered in the National Security Agency's (NSA) Acquisition Resource Center (ARC). You can register at https://www.nsa.gov/business/acquisition-resource-center/.

4.1.7 Applicants ***must*** maintain an accounting system capable of tracking the costs associated with the GenCyber grant accurately and adequately. Institutions must submit itemized invoices with invoice submissions.

4.1.8 Applicants ***must*** provide a certificate of liability insurance to document that student safety, liability, and insurance issues are addressed. This certificate ***must*** be included with the proposal. Please use the following address for the National Security Agency:

9800 Savage Road

Suite 6804

Fort George G. Meade, MD 20755

4.1.9 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.

4.1.10 Must any GenCyber activities funded by this NSA grant potentially be regulated as human subjects research (HSR), the activity shall comply with NSA/CSS Policy 10-10 and be designed and conducted to either: 1) not be HSR pursuant to NSA/CSS Policy 10-10, or 2) be exempt HSR pursuant to Part 219 of Title 32, Code of Federal Regulation.

4.1.11 Faculty (Principal Investigators/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.

SECTION V: 2021 GenCyber Grant Proposal Submission

5.1 Components and Deadline

Proposal submissions must include the following components: institutional data, all pages of the cover sheet, program narrative, budget with all supporting documentation, and all required government forms listed below. Please do not upload any zip or html files as there is a chance that they cannot be unzipped or opened on government systems.

5.2 Background Information on Institution

The proposing institution should respond to the information as requested by checking the appropriate box in each question. Information gathered in this section is used by the Program Office to respond to requests for information from federal partners and others.

5.3 Program Narrative

This section contains a series of narrative questions that allow the applicant to describe their proposed program. Detailed information regarding program narrative requirements can be found in Appendix B. **The Program Narrative is limited to 12 pages,** not including the Cover Page, Table of Contents or Reference pages. Letters of support are not necessary.

It is recommended to review the proposal evaluation criteria prior to and while preparing the program narrative section of your proposal. Please see Appendix A-C for more details.

5.3.1 Proposal Narrative Format

a) Proposal Narrative shall use 12-point Times New Roman font. When appropriate, respondents may use two-page foldouts, which will count as two pages for page limitation purposes. To assist the GenCyber staff with proposal review and evaluation, proposals shall include a Table of Contents which will be excluded from the page count. It is recommended to use the Table of Contents feature in Microsoft.

b) Page Setup Parameters:

- Paper Size, Width – 8.5”
- Paper Size, Height – 11”
- Margins (Top, Bottom, Left, Right) – 1”
- Gutter – 0”
- From Edge (Header, Footer) – 0.5”

5.4 GenCyber Program Budget

The Proposal Budget will justify all expenses required to achieve the program objectives. The budget and justification will cover personnel, consultants, equipment, supplies, travel and any other program expenses. It is encouraged that institutions budget for GenCyber branded items for participants. The budget can be accessed within the proposal submission site after you have registered for an account. Budget instructions are included as Appendix E within this document. Once all required information is entered into the site, budgetary information on the Proposal Cover Sheet will automatically be populated.

5.5 Proposal Structure

All submitted proposals must include the following:

5.5.1 All pages of the Cover Sheet will be automatically generated on the GenCyber Proposal Website when you are ready to submit your proposal. Please print, have an authorized representative sign, and upload to the proposal website. This form MUST BE signed by an authorized official at your institution.

5.5.2 Proposal Narrative (**12 pages maximum**) – Upload to GenCyber Proposal Website.

5.5.3 The required Office of Management and Budget (OMB) forms below can be found in the Submission Checklist of the GenCyber Proposal Website. Please download the forms, complete the forms, and have the forms signed by an authorized representative. After the forms are completed and signed, please upload them to the proposal website.

a) Budget Worksheet

b) Supporting Budget Documentation (i.e., quotes, payroll information)

c) Signed Application for Federal Assistance - SF424

d) Budget Information – Non-Construction Programs - SF424

e) Signed Assurances – Non-Construction Programs - SF424B

f) Signed Certification Regarding Lobbying Form

g) If lobbying is occurring, Disclosure of Lobbying Activity – SF LLL

h) Audit Report A-133 – (if you have a link/URL where report is posted, provide only the link. Otherwise, upload the document.)

i) Certificate of Liability Insurance

j)

5.5.4 Signatures from an authorized official are required on the Proposal Cover Sheet, SF-424, SF-424B and Certification of Lobbying.

5.6 Proposal Submission

After all required information is entered and uploaded into the proposal submission site, click the submit button for your proposal to be accepted into the system. Be sure you are ready to submit, as you will **not** be able to make any proposal changes, additions or deletions after submission.

5.7 Submission Deadlines

The proposal including all completed submission requirements, as outlined above in the Proposal Structure, must be submitted on the GenCyber Proposal Website (https://www.gen-cyber.com/host/) **by the submission deadline of 11:59PM Eastern Daylight Time on 2 April 2021 in order to be considered for a 2021 GenCyber Grant.**

Proposals received after this date/time will not be considered. Hardcopy proposals will not be accepted.

SECTION VI: 2021 GenCyber Grant Proposal Evaluation Criteria

6.1 Summary

6.1.1 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 and availability of funds.

6.1.2 The Government intends to evaluate proposals and make awards without discussions; however, the Government reserves the right to conduct discussions, at the discretion of the Grants/Contracting Officer. Due to the unique nature of each proposal, the Grants Officer may select one or more individual proposals for discussions. Selection of one or more proposals for discussion will not obligate the Government to enter into discussions with any other offeror.

6.1.3 The Government will award to the offerors whose proposal offers the **best value** in terms of the quality of the program in reaching GenCyber goals, diversity plans, cost-per-camp, cost-per-participant, curriculum, and outreach engagement. Additional factors that influence funding decisions include the geographic dispersion of all programs, the camp type, and the number of individuals and/or populations served by the program. For returning programs, previous track record of program performance and budgetary management will also influence funding considerations. In the absence of previous experience, evaluations will be based on the previously stated criteria. The best value selection is based on a determination of which proposal offers the best trade-off between price and the factors identified above, where those factors are considered an integral performance element.

6.1.4 The evaluation will be based on a complete assessment of the offeror's proposal.

6.1.5 Decisions to fund selected proposals will be based on the selection criteria already identified and funds availability. 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 cybersecurity education, then funds availability alone will be the determining criterion for award. Prior GenCyber Grantee status does not assure a 2021 grant award.

6.1.6 Determining how well the offeror's proposal meets the solicitation

requirements will be accomplished in the following steps.

a) A determination will be made if the offeror's proposal meets the solicitation eligibility requirements. Those that do not meet eligibility requirements will be disqualified from consideration. The requirements are listed in Section 3.0 but also include requirements listed in this CFP such as inclusion of 30 instructional hours (along with the required pre/post camp outreach hours), use of a K12 classroom teacher, and curriculum that contains ALL of the Concepts or Principles along with cybersafety and cyber ethics.

b) Discriminators will be identified for the proposals reflecting the unique strengths, weaknesses, significant weaknesses, and deficiencies of each proposal.

c) The discriminators will be totaled to determine an overall technical rating.

d) The overall technical rating will be evaluated alongside the pricing for a best value determination.

e) Factors such as geographical location, abundance of resources/other activities in the area, program type, past performance of the submitting institution, uniqueness of proposal, etc. may also factor into final funding decisions.

6.1.7 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.

6.2 Proposal Processing and Review Instructions

Proposals received by the GenCyber Program Team are assigned to the program for acknowledgement and, if they meet the solicitation requirements, for review. All proposals may be carefully reviewed by a team of Subject Matter Experts consisting of an assessment team of individuals with pedagogy and cybersecurity expertise in the particular programs represented by the proposal. A team of government reviewers will carefully review each eligible submission. Care is taken to ensure that reviewers have no conflicts of interest with the proposal. The contractor assessment team may make recommendations for award. The Government conducts an evaluation of all eligible proposals and will make final selection. The government does not guarantee written feedback on any proposal submission.

6.3 Notification of Award

Notification of award is made to *the submitting organization* by the National Security Agency. Organizations whose proposals are declined will be advised as promptly as possible by the GenCyber Program Team. Please note that notification of award does not constitute an award document. Do not make any purchases until you receive an official, signed grant award from the Maryland Procurement Office.

6.4 Award Conditions

6.4.1 The National Security Agency's award consists of:

a) The award notice, which includes any special provisions applicable to the award and any numbered amendments thereto;

b) The budget, which indicates the amounts, by categories of expense, on which National Security Agency has based its support (or otherwise communicates any specific approvals or disapprovals of proposed expenditures);

c) The proposal referenced in the award notice;

d) The applicable award conditions, such as Grant General Terms and Conditions; and

e) Any announcement or other National Security Agency issuance that may be incorporated by reference in the award notice.

6.5 Other Information

All those who are awarded grants must be aware of the Freedom of Information Act (FOIA). Must a FOIA request be submitted to the National Security Agency, your proposal would be subject to disclosure.

SECTION VII: Post-Grant Award Requirements

7.1 As required by OMB, the following forms ***are required after grant award***. The forms may be found at: https://www.grants.gov/web/grants/forms/post-award-reporting-forms.html.

7.1.1 Request for Advance or Reimbursement SF-270 (OMB Number 4040-0012) (must be submitted with your invoice).

7.1.2 In addition to the SF-270, the following steps are required for electronic invoicing:

a) Registration in SAM (System for Award Management) at https://www.sam.gov

b) Registration with the NSA ARC at https://www.nsa.gov/business/acquisition-resource-center. If you have any problems with the site, please call (866) 914-6272.

c) Obtain an ECA Medium Assurance Certificate through either ORC, Identrust, or DoD. The certificate comes 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. The cost ranges from $100 - $300 per year. The grantee may be asked to provide personally identifiable information such as a social security number. This information is not released to NSA and only stays with the certificate issuer. This process normally takes 1 to 2 weeks. The Government suggests that you start the ECA process once you have been awarded an FY20 GenCyber Grant.

d) 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. In order to set-up your account correctly, please let the MPO office know that this account will be for a grant and not a contract. Additionally, if your institution's invoices are administered by the Office of Naval Research (ONR), please inform the MPO Help Desk which regional ONR Office invoices must be routed.

e) The grantee receives a welcome email entitled "Welcome to the MPO Web Site" that includes their user id, password, and instructions on getting started.

7.1.3 After grant award and if needed, budget modifications must be requested and submitted to the GenCyber Program Team at GenCyber@nsa.gov.

7.1.4 Federal Financial Report SF-425 (OMB Number 4040-0014) Required to submit with final invoice.

7.1.5 Tangible Personal Property Report SF-428 (submit when equipment/supplies have a current per unit fair market value of $5,000 or more. Any equipment/supplies that has a current per unit fair market value of $5,000 or less, shall remain the property of the institution and shall be dispositioned as the grantee deems fit to further the GenCyber Goals).

7.1.6 Tangible Personal Property Report Annual Report SF-428-A

7.1.7 Tangible Personal Property Report Supplemental Sheet SF-428S

7.1.8 Tangible Personal Property Report Final Report SF-428-B (Required for closeout of grant)

7.1.9 Tangible Personal Property Report Disposition Request/Report SF-428-C (Property forms may be found at: https://www.grants.gov/forms/post-award-reporting-forms.html)

7.2 The following deliverables ***are required*** as a condition of all GenCyber grant awards:

7.2.1 All Camp Reports (additional guidance will be provided in the Program Director's Guide).

7.2.2 Itemized invoices submitted along with each invoice.

7.2.3 Surveys provided by Program Office or program support (required to be completed as requested throughout the grant award period).

7.2.4 Lessons Plans on the GenCyber provided template (3 lesson plans are required to be submitted with Camp Final Reports).

a) All lesson plans and associated deliverable material (e.g., documentation or information technology) may be made publicly available by the U.S. Government or by others to further federal purposes.

b) All lesson plans, delivered materials, documentation and information technology will meet the NSA ICT Accessibility Standards, derived from Section 508 of the Rehabilitation Act (29 USC 795d) and Web Content Accessibility Guidelines 2.0 AA requirements.

7.3 The Offeror shall follow the guidance provided within the NSA ICT Accessibility Standards and the NSA ICT Accessibility Score Sheet to conduct a self-evaluation of their course materials, and vendor delivered information technology (software and hardware). The Offeror shall identify how materials, documentation, and information technology can be interacted with the keyboard only, a third-party screen-reader (JAWS or NVDA), and that no information/instruction is presented in single-sense format only (auditory, color, visual, etc.), through the completion of the self-evaluation. Additionally, if the Offeror's individual criteria scores fall below a 5.0, they

shall provide documentation regarding those criteria, why they fail, the deliverables negatively impacted, how it will effect end-users, and a procedure and report that demonstrates how they plan to remediate or alternatively meet the Agency Accessibility Standards.

The Offeror shall document and demonstrate any instance where the NSA ICT Accessibility Standards and Score Sheet Requirement are not directly applicable to the ICT under procurement. If the Offeror demonstrates non-applicability, they must document how the ICT meets the NSA ICT Fundamental Accessibility Requirements. If they are unable to demonstrate for all fundamental requirements, they shall provide documentation regarding those criteria, why they fail, the deliverables negatively impacted, how it will affect end-users, and a procedure and report demonstrating how they plan to remediate or alternatively meet the Agency Fundamental Accessibility Requirements. All RFP response documentation delivered will also be produced in an accessible format that meets the NSA ICT Fundamental Accessibility Requirements, and will additionally be available in braille format, upon request.

7.4 All lesson plans and associated deliverables will be delivered with the following rights to the government. The U.S. Government reserves a royalty-free, nonexclusive and irrevocable license to reproduce, publish, or otherwise use the work for Federal purposes, and to authorize others to do so. Strengthening the Nation's cybersecurity, particularly through cybersecurity education at all levels of education to foster the knowledge and skills of individuals who may ultimately join the U.S. Government, is an important Federal purpose. The U.S. Government has the right to authorize others to reproduce, publish, and use these materials in furtherance of this Federal purpose. Furthermore, the Government does not have a legal objection if the curricula is provided with the Creative Commons Attribution 4.0 International License.

Appendix A

Proposal Narrative Outline

The following guidance must be used for all Student, Teacher, Combination, and "GenCyber Goes Virtual" proposals

Section I: Introduction

Section II: Target Participation/Recruitment/Enrollment

1. Targeted participants
2. Marketing/Recruitment
3. Enrollment/Retention

Section III: GenCyber Program Overview and Timeline

1. Proposed Program Overview
2. Proposed Pre/Post Camp Outreach
3. Program Timeline

Section IV: Learning/Assessment/Legacy/Curriculum Delivery/Reflections

1. Learning
2. Assessment
3. Program Legacy
4. Reflections (previous participants only)

Section V: Program Personnel and Faculty Qualifications

1. Program Personnel

Section VI: Summary

Appendix B

Proposal Narrative

The narrative represents allows you to describe your proposed program in 12 pages. Institutions must clearly address the respective program questions and demonstrate their ability to be successful in the stated objectives for Student, Teacher, or Combination Programs, or the "GenCyber Goes Virtual" Teacher Camps. Appendix C contains guidance for GenCyber Capacity-Building Activity submissions. The narrative for any submitted proposal should be both detailed and concise.

Program narratives should adhere to the following format. Failure to adhere to this format may result in a proposal not being reviewed. This format matches with the proposal review rubric used for all submissions.

Section I: Introduction

1. Briefly describe the proposing institution's qualifications and desires to work in the K12 environment.

2. Include a brief description of the local K12 cybersecurity ecosystem.

3. Describe how will the program help participants learn and understand GenCyber program goals? How will this proposed program further develop cybersecurity education at the K12 level?

Section II: Target Participation/ Recruitment /Enrollment

1. **Target Participation:** Describe the participants you anticipate will enroll in the program. This must include information such as socio-economic status, gender, ethnicity, cybersecurity and computer knowledge/experience, grade level(s), and prior GenCyber program participation.

    a. Justify the targeted number of participants. Include estimated demographic data.

    b. Anticipate the number of returning GenCyber participants you will accept. If you predict a high number of returning GenCyber participants, explain how you will adjust the camp schedule to this audience to ensure they are learning new and more advanced material.

    c. Include a description of the program diversity goals.

2. **Marketing/Recruiting:** Describe how you will publicize and market your program to recruit the targeted participants.

a. How will the program attract/recruit diverse participants? GenCyber aims to serve a diverse population in terms of ethnicity, race, gender, special needs, socio-economic status, and/or geographic location.

b. How will you ensure that all events are branded as GenCyber events?

3. **Enrollment/Retention:** Include a brief description of the selection process of participants. Include a description of your retention plan to ensure that participant numbers are being met and maintained.

    a. How will participants be selected?

    b. Teacher programs: Include plans for requiring teachers to submit a letter of approval from school administration.

    c. How does the retention plan specifically relate to your target participants? The target audience, recruitment strategy, and retention strategy must all be interrelated.

4. **Format:** Include a description of the program format. Be sure to include details on how the proposed format will accomplish GenCyber program goals. For example, increasing interest in a virtual environment is difficult if technical issues prevent a participant from completing activities. The proposal should address these sorts of challenges and offer methods to overcome.

Section III: GenCyber Program Overview and Timeline

1. Proposed Program Overview: Outline the program and describe how it will address the GenCyber program goals, cybersecurity ethics, and GenCyber Cybersecurity First Principles and/or Concepts.

a. GenCyber Cybersecurity First Principles & Concepts: Each GenCyber Program must specifically state which framework and corresponding Cybersecurity Concepts and/or First Principles will be included in the curriculum. Provide a rationale for the proposed framework and its relevance for the intended program participants given their ages, backgrounds, interests, etc.

The proposal must demonstrate how the camp curriculum will use the selected Concepts or Principles throughout the curriculum and outline how the various lessons (e.g., cryptography, Python programming, drone hacking) are unified by the chosen curriculum

concept(s). Utilizing the Principles or Concepts to teach cybersafety is highly encouraged. The curriculum must emphasize the explicit and implied relationship among different concepts and the lessons. By making explicit connections among topics, participants are more likely to leave the program where the "whole" of what they now know is greater than the sum of the parts. Aligning the curriculum with local factors is also encouraged. Including cyber ethics is considered a foundation of all GenCyber activities.

b. **Post-Secondary and Career Awareness:** Explicitly describe how participants will be made aware of opportunities in the field of cybersecurity. Consideration of factors such as the target audience and local cybersecurity landscape should be considered.

2. **Proposed Pre/Post Camp Outreach:** Describe how the pre/post camp events will develop and/or continue engagement beyond the summer camp experience. Due to the extremely competitive nature of the GenCyber program, it is encouraged that all proposals contain concise details on program happenings.

3. **Program Timeline:** Include a timeline of proposed events (pre/post camp outreach + summer camp activity) including a brief description of the event and the format of the event. Include the number of instructional hours that will occur during each event.

Section IV: Learning/ Assessment/ Legacy / Curriculum Delivery / Reflections

1. Learning: Specify all content as it relates to lessons and activities and their relevance to the GenCyber Concepts or Principles.

a. Include a schedule for the 30-hour summer camp. The schedule must include time frames, topics, activities, cyber ethics, and relation to Concepts/Principles.

b. In order to be considered, at least 30 instructional hours must be included. Proposal must note the total number of instructional hours.

c. Explain how the curriculum will facilitate a learner-centered classroom.

d. Include curricula and instructional materials appropriately designed and presented for age-appropriate education. Examples of reliable technology used to augment the GenCyber goals include but are not limited to Raspberry Pi's, Spheroes, Flash drives loaded with software and/or activities, cyber ranges, and curriculum, curriculum frameworks, and K12 resources for teacher participants.

e. How does the proposed curriculum/activities relate to the target audience and address GenCyber program goals?

2. Assessment: Describe the process you will use to show that each participant has met the goals of the program. The classroom teacher uses formative assessment of student performance during the course of the lesson to adjust instruction as needed. This same philosophy must be used in a camp environment.

a. How will you ensure that all participants (regardless of background and experience) will acquire new learning as a result of their participation in this program?

b. What methods of differentiation are used in each activity to ensure learning?

c. How will all participants receive feedback on learning after completing activities?

d. How will all participants be given opportunities to reflect on their learning experiences?

e. How will you ensure that the teacher participants will grow professionally as a result of their participation in this program? What actions will help lead to higher Teacher Readiness scores?

3. **Program Legacy:** Describe the connections you will and/or have established in your community as a result of the GenCyber program to grow interest among parents, local school systems, and other stakeholders in continued cybersecurity education at the local level program. Describe how the program will foster continued cybersecurity awareness in the community.
    a. Student programs may choose to describe items such as club developments, local community projects, increased enrollment in college/community college degree programs, etc.
    b. Teacher Programs may describe ways in which your program helps teachers become GenCyber leaders through applied, practical, or project-oriented activities or the development of Teacher Learning Communities.
    c. Include descriptions of community partners or the ways in which this GenCyber project has the potential to impact the local community (past, present, future).
4. **Reflection of Previous 2020 GenCyber Programs Only.** List the challenges and recommendations provided in your 2019 or 2020 site visit report. Explain how you will address each recommendation.

Recommendation/Challenge	How will you address each recommendation?
Recommendation 1	We will address recommendation 1 by…
Recommendation 2	We will address recommendation 2 by…
Recommendation 3	We will address recommendation 3 by…

Section V: Program Personnel and Faculty Qualifications

1. Program Personnel: Provide information on the personnel who will be charged with implementing your proposal. Each camp is required to have a designated Program Director and Lead Instructor, defining the duties and responsibilities between two different individuals. Each camp is also required to have a K-12 pedagogical expert on the camp staff to assist with curriculum development/ review/delivery. This person must have K12 classroom experience. Institutions must consider the target audience when selecting all camp staff. Proposals that include multiple camp administrators (who have little to no contact with participants) may not be

considered as the purpose of the camps are to engage with target participants.

a. Provide Program Director and Lead Instructor's Name, Qualifications, Major responsibilities, and corresponding qualifications, experience, and/or training to teach camp coursework. Lead Instructors must have experience as an instructor in a formal education setting – i.e., college classroom, K-12 classroom.
b. Describe the major responsibilities of the personnel in your program, and explain previous qualifications, experience, and/or training that qualifies them for their positions. Be certain that the connection between responsibilities and qualifications is clear.
c. Include an overall staff to student ratio. Guest speakers and similar individuals must not be included in staff: student ratio.
d. Include a brief list of guest speakers and how he/she/they relate to GenCyber program goals.
e. Describe any professional development activities for the instructional staff - pre-program, during camp and/or post camp.

Section VI: Summary: Include a brief program overview to include the institution, program name, and highlights of the program. The summary must be 200 words or less. If funded, this summary is used for promotional purposes in events such as the Spring/Fall meetings.

Appendix C

GenCyber Capacity-Building Activity

Proposal Narrative

The narrative allows you to describe your proposed program or project under the GenCyber Capacity-Building aspect of the CFP. The Program Office is interested in creative and unique ideas that impact on a regional or nation-wide scale. Projects must further the goals of the GenCyber program and allow participants to continue to build interest in cybersecurity skills and careers beyond an existing GenCyber experience. Proposals must not rely on the successful funding of other projects (i.e a GenCyber student program). The narrative for any submitted proposal should be both detailed and concise.

Program narratives should adhere to the following format. Failure to adhere to this format may result in a proposal not being reviewed. This format matches with the proposal review rubric used for all submissions.

Section I: Introduction

1) Briefly describe the proposing institution's qualifications and desires to work in the K12 environment.
2) Include a brief description of the local K12 cybersecurity ecosystem.
3) Describe how the project will help participants learn and understand GenCyber program goals? How will this proposed program further develop cybersecurity education at the K12 level?

Section II: Target Participation/ Recruitment /Enrollment

1) **Target Participation:** Describe the participants you anticipate will benefit from the propose project. This must include information such as socio-economic status, gender, ethnicity, cybersecurity and computer knowledge/experience, grade level(s), and prior GenCyber program participation.
    a) Justify the targeted number of participants.
    Include estimated demographic data on participants.
    b) Include a description of the program diversity goals.
2. **Marketing/Recruiting:** Describe how you will publicize and market to recruit the targeted participants.
    a) How will the program attract/recruit diverse participants? GenCyber aims to serve a diverse population in terms of ethnicity, race, gender,

special needs, socio-economic status, and/or geographic location.

b) How will you ensure that all events are branded as GenCyber events?

Section III: GenCyber Program Overview and Timeline

1) **Proposed Program Overview:** Outline the project and describe how it will address the GenCyber program goals, cybersecurity ethics, and GenCyber Cybersecurity First Principles and/or Concepts. If the program involves a virtual environment, describe how the proposed program will accomplish/advance the goals of the GenCyber program.
2) **Program Timeline:** Include a timeline of proposed project that includes development, implementation, and assessment phase.

Section IV: Learning/ Assessment/ Legacy

1) **Learning:** Specify all content as it relates to lessons and activities and their relevance to the GenCyber Concepts or Principles.
    a) Include a discussion of how the project will further develop the K12 cybersecurity education ecosystem. Include specific examples to support the impact the project could have on a local area, the nation, or the GenCyber community.
2) **Assessment:** Describe the process you will use to show that the project has met the pre-determined impact goals.
3) **Program Legacy:** Describe the connections you will and/or have established in your community as a result of this GenCyber project to grow interest among participants at the K12 level. Describe how the program will foster continued cybersecurity awareness.

Section V: Program Personnel and Faculty Qualifications

1) Program Personnel: Provide information on the personnel who will be charged with implementing your proposal. Each camp is required to have a designated Program Director. Each project is also required to have a K-12 pedagogical expert on the staff to assist with development/delivery/etc. This person must have K12 classroom experience. Institutions must consider the target audience and project purpose when selecting all camp staff.
    a) Provide Program Director name, qualifications, major responsibilities, and corresponding qualifications, experience, and/or training.
    b) Describe the major responsibilities of the personnel in your program, and explain previous qualifications, experience, and/or training that qualifies them for their positions. Be certain that the connection between responsibilities and qualifications is clear. Include staff member with K12 experience and role of this individual.
    c) Describe any professional development activities for the staff.

Section VI: Summary: Include a brief project overview to include the institution, program name, and highlights of the project. The summary must be 200 words or less. If funded, this summary is used for promotional purposes in events such as the Spring/Fall meeting

Appendix D

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.

Additionally, it is a program requirement that conversations on ethics and the ethical responsibilities of cybersecurity professionals form a foundation of all camps.

Appendix E

2021 GenCyber Budget Instructions

The purpose of the budget is to present and justify all expenses required to achieve your program objectives. All costs must be reasonable and allowable. The budget and justification must cover personnel, consultants, equipment, supplies, travel, and any other program expenses. Budgetary information shall be entered into the GenCyber Proposal Submission site through your account; and cover sheet budgetary information will be automatically populated. All information provided in the budget shall be found within the proposal and/or readily available online with direct links to the information. Please be aware that if awarded a grant, there will be no period of performance extensions beyond the two-year timeframe.

Before starting your budget, please obtain and have all supporting budget documentation for upload into the system. Supporting budget documentation must include quotes for supplies, materials, travel, rental fees, contracted staff, and indirect rate agreements. If any expenses in your proposed budget are over $200, quotes are required to be uploaded into the proposal submission site. Additionally, in accordance with 2 CFR 200.404, the Government requires the proposer to submit documentation validating all personnel salaries that are listed in the proposed budget. (Please note that the aforementioned list is not all-inclusive.) Must supporting budget documentation be missing and/or blank documents received, your proposal package may be ineligible for evaluation and consideration for award.

Your GenCyber budgets will be subject to rigorous scrutiny and may be subject to audit. Therefore, we strongly recommend that you be thorough in the development of your budget. It is **mandatory** that all sections are completed with the categories that suit your program's characteristics. An explanation of each item is required; leaving the explanation blank may cause your budget to be rejected. Institutions are encouraged to itemize as much as possible and include descriptions and quotes as needed. Proposing institutions are encouraged to be as cost efficient as possible while also ensuring a safe, engaging, and fun experience for campers!

Please note that the following costs are **Not Allowed** and must not be included in proposals:

- Monetary gifts, gift cards, gift certificates and/or payments to attend camp for student participants.
- Gifted laptops (or devices of similar value) intended for **students** to keep after the program has ended.

- Proposal writing expenses.
- Any professional development conferences/meetings other than the GenCyber Spring or Fall Meetings.
- Deposits or fees intended to hold a seat or "save a spot" in the program and guarantee student's attendance and/or program completion.
- Stipends for student participants (Regardless of the funding source).
- Travel allowances for student program participants except for daily local commuting. Transportation for students should be done in the form of a prepaid pass or a bus rental fee. Student participants should not receive cash for transportation.
- Course fees, certification textbook/exam fees, and/or tuition reimbursement. Exceptions to this will be considered on a case-by-case basis. Please include justification of these expenses.
- Graduation student tuition reimbursement is not allowed under a GenCyber grant. Graduate students may be paid an hourly rate but GenCyber camps/events are not research projects nor are they teaching assignments.

Section A	Description	Example/Budget Line
Employees	Lists all employees working with your program who will be on payroll during the dates of the program. The program director and lead instructor must be mentioned by name. You may refer to other employees by name. However, it is acceptable to list an employee as "to be determined." Proposals that include high numbers of admin support staff who have little to no contact with participants are discouraged. Show how you calculate the salary or rate for each employee. In order to support the reasonableness of the personnel costs proposed, in accordance with 2 CFR 200.404, the Government will require the Grantee to submit documentation validating all personnel salaries that are listed in the proposed budget.	• Joe Cyber, Program Director • Dr. Pi, Lead Instructor • Instructor • Teaching assistants • Camp Counselor The documentation may be provided in a variety of forms, listed by preference below: • A copy or screen shot of the HR payroll information or a copy of a paystub. Please note – may be redacted for PII concerns • Publicly published pricing for same or similar services (i.e., comparable pricing that is available for all to see). Provide a brief explanation of the relationship between the proposed cost and the supporting data • Recent invoices for same or similar services

Section A	Description	Example/Budget Line
Benefits	In this area, include employee payroll benefits. Please list out all benefits and include the benefit rates. Also, show and explain how you calculated each benefit. If you have a question about benefits, contact your institution.	• Health Insurance • Life Insurance
Section B		
Indirect	Indirect costs are actual costs incurred to conduct the normal business of an organization that is not readily identified with, or directly charged to, a specific project or activity. These costs are incurred for common or joint objectives and therefore cannot be readily identified with a specific project or activity of an organization. Typical examples of indirect costs are the costs of operating and maintaining facilities, local telephone service, and account services. Supporting documentation shall be provided in the form of a Department of Health and Human Services (DHHS) Rate agreement or any other previously negotiated for fringe benefits. If your organization does not have a federally negotiated rate, please provide a detailed breakdown of each expense incurred as an indirect cost. The appropriate F *Insurance refers to additional coverage purchased specifically for the duration of the program.	• Clerical Support • Janitorial Staff • Security Staff • PKI/Token • Insurance* • F & A rates must include documentation of all 3 levels; with justification as to why the level submitted was chosen. (Example: face to face summer camps on campus must have a different F & A rate as a virtual camp). • Teacher stipends and other participant costs must not be considered when calculating the F & A fees.

Section B	Description	Example/Budget Line
Indirect - Third-party services	This section shall include program-related costs for services provided by a third-party contractor or vendor.	• Seasonal internet or software usage • Printing services
Section C		
Contracted staff	Include any personnel who will work for your program and will not be on your institution's payroll during the dates of the program. Show the calculation and provide an explanation for each of the personnel listed. No benefits may be charged to the grant for contracted employees or consultants.	• Guest Speakers • Student Mentors • Industry Experts • K12 staff
Section D		
Travel	Include your estimated travel expenses pertaining to the GenCyber meetings (3). Attendance is mandatory for the program director and lead instructor. Institutions may elect to budget for ONE teacher participant to attend ONE fall meeting. This person does not replace the PD/LI attendance requirement. Additionally, list any other travel costs that are **not** related to the GenCyber spring and fall meetings. • Field trips are allowed during the instructional day. Travel allowance for local commuting is permitted (i.e., providing a bus at a central location for students). • Travel reimbursement for travel to a program site are only permitted for teacher programs as part of a stipend.	Budget for meeting costs in Spring (April)/Fall (Sept) to Baltimore area • Vehicle Rental • Parking • Guest Speaker Travel • Metro/Subway Fare Cards (No cash) • Teacher Participant Travel Allowance as part of Stipend *Travel for professional development conferences is **NOT** allowed (e.g., National Initiative for Cybersecurity Education Conference).

	(Note: Perdiem costs may not exceed GSA rates for each location – rates can be found at https://www.gsa.gov/travel/plan-book/per-diem-rates and select 2021/22 fiscal year.)	
Section E	**Description**	**Example/Budget Line**
Facilities	In this category, list costs related to the rental of space for your GenCyber program. Show the calculation and provide an explanation for each item entered.	• Classroom rental • Building rental
Section F		
Supplies-Classroom	This section shall detail the cost of any supplies or teaching materials that may be used in the classroom by the instructor. Please provide detailed information on the price and quantity of each item to be purchased.	• Textbooks • Workbooks • Software, educational technology and licenses • Games • Classroom Posters
Supplies - Office and administrative	This section shall include all supplies regularly used to support the program. Please provide detailed information on the price and quantity of each item to be purchased.	• Postage • Paper • Post-Its • Binders • Printer Ink

Supplies - Miscellaneous	Include any other supplies that will be purchased by the program that do not fit into any of the supply categories. The expenses in this category need to be detailed. Please avoid general terminology such as "other." *Please note that the GenCyber Logo will be provided to each program and shall be used on promotional items and giveaways.	• Participant T-shirts • Completion Certificates • Promotional Items • USB Flash Drives **Gift cards and/or gift certificates are not allowed**

Section F	Description	Example/Budget Line
Equipment	Equipment is defined as an item of property that is electronic and has an expected service life of more than one year. Detail all equipment purchases. Student participants may be provided equipment such as Raspberry Pis or Arduinos to continue their interest and learning in the GenCyber subject areas. (Each student participant is limited to a **total of $125** in take-aways – to include technology items and GenCyber swag.) Proposals that exceed this amount will be asked to re-submit or may not be considered. Student participants may **not** be provided with equipment such as laptops, Chromebooks, iPads or Tablets to take with them at the conclusion of the program. Equipment may be purchased and provided to teacher program participants for the specific purpose of implementing lessons/curriculum or as a resource for teaching GenCyber subject areas. (Each teacher participant is limited to a **total of $350** in take-aways – to include technology items and swag.) Proposals that exceed this amount will be asked to re-submit or may not be considered.	• Computer Kits/Parts • iPads/Tablets *(Classroom use or Teachers Only)* • Laptops *(Classroom use or Teachers Only)* • Raspberry Pis • Arduino • Drones • Robotics • Digital Cameras • The purchase of furniture is **not** allowed.
Section G		

Other Expenses	In this section, include any proposed expenses of the program that do not fit into any of the other defined categories. A detailed explanation is required to demonstrate that costs are not duplicated elsewhere in the budget Food and refreshment are only allowed during the instructional hours of the camp (unless residential camp).	• Meals (breakfast, lunch, dinner) • Snacks • Entrance Fees for Field Trips • Advertising Costs
	Field trips are allowed only during the instructional day. Gift card, gift certificates, and/or money for the purpose of awards to participants are **NOT** allowed. The GenCyber Program wants participants to be a part of the program because they are interested in the camp and want to learn versus the "freebies." Deposits or fees collected from participants to hold a seat or "save a spot" in the program or guarantee student attendance and/or program completion are **NOT** allowed. This also includes fees that would be reimbursed after participants show up and/or complete the camp. Additionally, a fee **cannot** be charged to participants for the purpose of expanding your program. Your program must stand within the constraints of your grant dollars. If you wish to expand your program over and above what the grant funds, you must find an additional funding source.	

Other Expenses – Tuition, Fees and Participant Costs	A detailed explanation is required to demonstrate that costs are not duplicated elsewhere in the budget. Teacher stipends must provide a breakdown of the expenses included in the stipend total (i.e., cost of lodging, cost of travel, % of teacher salary for a specific school district). All estimated stipend costs must include a quote and/or documentation to justifying the amount(s). Student stipends for attending a GenCyber camp are **not** permitted regardless of funding source.	• Stipends (*for teacher participants only*) • Evening and weekend activities • Supplies given to participants • Include an estimated monetary total of the overall supply value given to participants.