2020 GenCyber CFP – Table of Contents

(Revision 20191002a)

2020 GenCyber Grant Call for Proposal Overview

The National Security Agency's National Cryptologic School in conjunction with the National Science Foundation has a requirement to provide cyber 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 or commuter learning events (ex. summer camps held during May-September timeframe) for students; and providing instruction, instructional materials, and effective teaching methods to 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 university, public or private school and that academic institution will have to be apply. The goals of the program are to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the Nation, help all students understand correct and safe on-line behavior, and improve teaching methods for delivering cybersecurity content in K-12 curricula.

GenCyber Vision

"INSPIRING THE NEXT *GEN*ERATION OF *CYBER* STARS"

Our vision is for the GenCyber program to be part of the solution to the Nation's shortfall of skilled cybersecurity professionals. Ensuring that enough young people are inspired to direct their talents in this area 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. To ensure a level playing field, GenCyber camps are offered at no cost to all student and teacher participants.

Funding Organization

GenCyber is funded by the National Security Agency (NSA) and the National Science Foundation (NSF).

Grant Award Information

1. GenCyber grant awards are anticipated to be up to $100,000 each. Programs with certain unique program circumstances may exceed that amount, based on the type of program and number of participants.
2. Due to the increased interest in the GenCyber program, grant award competition has increased. Accordingly, prior GenCyber grantee status does not assure a 2020 grant award.
3. Grant awards are **anticipated** to be announced in February 2020 with funding awarded in March 2020. Grant awards are effective for one year from the date awarded.
4. Please be aware that if awarded a grant, there will be no period of performance extensions beyond the one-year timeframe.

GenCyber Program Description

GenCyber Goals

The primary purpose of the GenCyber program is to support the growth of the next generation of cybersecurity experts for the nation.

- Increase interest in cybersecurity and diversity in the cybersecurity workforce of the Nation.
- Help all students understand correct and safe on-line behavior.
- Improve teaching methods and cybersecurity content for K-12 curricula.

GenCyber Programs Offered

The 2020 GenCyber Program has two program options for which grants are awarded:

- **Student Programs** – Student programs provide age-appropriate cybersecurity awareness learning opportunities for K-12 students in a standards-based and organized curriculum promoting the GenCyber Cybersecurity Concepts and/or GenCyber Cybersecurity First Principles, online safety, and ethics.
- **Teacher Programs –** Teacher programs provide a comprehensive experience involving practice in implementing the GenCyber Cybersecurity Concepts and/or GenCyber Cybersecurity First Principles, ethics, and opportunities for classroom observations and practicum involving hands on experiences. These programs should include helping teachers with the preparation of cybersecurity lesson plans designed for teachers to take back to their classrooms.

If you intend to conduct two separate types of camps (i.e., Student and Teacher), you must submit **separate** grant proposals for **each** camp. Multiple camps of the same camp type using **different** curricula (i.e., Beginner and Advanced) must submit **separate** proposals. Multiple camps of the ***same*** type using the ***same*** curriculum may be submitted on one proposal. Each proposal will be evaluated separately; therefore, one proposal should not be dependent upon another in any way.

GenCyber Camp Duration and Timing

1. GenCyber camps are expected to run a minimum of one week to include at least 30 instructional hours. Instructional hours are defined as those blocks of time in which students are actively engaged in learning (lecture, guest speakers, labs, hands-on activities, field trips, etc.). Breaks and lunch breaks that do not include educational activities are not included in the 30 hour minimum. It is recommended that students receive multiple breaks throughout the day and at least 30 minutes of uninterrupted lunch. Programs less than five days are generally insufficient to adequately meet the goals of the program. GenCyber camps are not intended to be conducted solely as preparation for cyber competitions.
2. GenCyber programs are primarily summer programs. However, adding follow-on instruction or activities (i.e. webinars, one-day events, etc.) to retain or advance the

participants' learning beyond the summer program is strongly encouraged.

3. When scheduling GenCyber summer camps, consideration should 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). For new GenCyber participants, be aware there is a lot of planning and preparation involved in conducting a camp, and you might want to consider scheduling your camp in July or August.

GenCyber Cybersecurity First Principles & Concepts

The GenCyber 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 should discuss how the various lessons (e.g., cryptography, Python programming, drone hacking, basic digital forensics, cyber crime, or network defense and attack) are unified by the chosen curriculum framework.

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

GenCyber Cybersecurity First Principles:

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

GenCyber Cybersecurity Concepts:

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

GenCyber Meetings

1. The GenCyber program holds two meetings each year for the Program Directors and Lead Instructors. The Spring Meeting kicks off the GenCyber Program year and provides an

overview of the GenCyber Program and guidance to Program Directors and Lead Instructors. This meeting also provides networking opportunities to learn about other institutions' programs and experiences. The Fall Meeting is held to bring together all of the programs to share best practices and lessons learned.

2. The 2020 GenCyber Spring and Fall Meetings will be held in the Baltimore/Washington Metropolitan area. The Spring meeting will be in late April/early May and the Fall meeting will be in mid/late September.
3. Program Director and Lead Instructor (or their proxies as approved by the GenCyber team) are **required** to attend both 2020 GenCyber meetings.
4. Proposal budgets must include travel costs for both the Program Director and Lead Instructor from each camp to attend these meetings.

GenCyber Curriculum

The GenCyber Program Team does not provide curriculum. Each institution is responsible for developing a creative and age appropriate curriculum that addresses the GenCyber First Principles and/or Concepts while advancing the goals of the GenCyber program. Included in Appendices D and E are Student and Teacher Program Curriculum Companion Guides to assist in your curriculum development.

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) developed for the GenCyber summer camps be delivered with final reports at the end of your program. These lessons plans will be shared publicly to further the goal of improving teaching methods for delivering cybersecurity content in K-12 curricula. 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 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 (see pages 18-19 for more detail).

Site Visits

The GenCyber Team will send representatives to observe one day of your camp. The site visit generally occurs on day three of an institution's camp offering. Observations are used to compose a final report of the 2020 GenCyber program and bring forth new ideas and suggestions to the Fall Meeting.

Surveys

Surveys are distributed to Program Directors for participants to fill out on the last day of camp. The surveys are specific to which type of camp you are offering. The purpose of the student end-of-camp survey is to assess interest in cybersecurity and report on GenCyber's first goal of increasing 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. Responses from the student surveys also provide suggestions for improving each camp to promote interest development.

The purpose of the teacher end-of-camp survey is to assess teaching/coaching readiness in order to report on GenCyber's third goal of improving teaching methods and cybersecurity content for K-12 curricula. The teacher end-of-camp survey looks at each GenCyber camp as a Professional Learning Community and provides an assessment of teacher readiness to teach/coach cybersecurity. In this report, 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.

2020 GenCyber Grant Proposal Eligibility Requirements

All Programs

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

1. Institution applying must be a university, public or private school or school system.
2. All program/camp titles must include the name GenCyber. For example, University A GenCyber Teacher Camp or Community College A GenCyber Academy.
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. A FICE (Federal Interagency Committee on Education) number must be included in college/university proposals, should your institution have one of these numbers. Institutions other than colleges and universities are not required to include a FICE #.
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
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/.
7. Applicants ***must*** maintain an accounting system capable of tracking the costs associated with the GenCyber grant accurately and adequately.
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

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.
10. Should any GenCyber activities funded by a 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 Regulations.

The GenCyber Program includes two different types of programs. Below are requirements specific to each program:

Student Programs

1. Proposals ***must*** indicate the capability to offer age-appropriate standards and performance-based cybersecurity learning summer programs in a safe environment for students in elementary, middle, and/or high school, as appropriate.
2. Utilizing K-12 pedagogical expertise in the curriculum development is required .
3. All student program participants ***must*** reside in the United States and be enrolled in a United States school or home-schooled.

Teacher Programs

1. Proposals ***must*** indicate the ability to train teachers in cybersecurity (to include Cybersecurity First Principles or Concepts) and provide them the knowledge and tools to prepare curriculum designed for teaching cybersecurity.
2. All teacher programs must ensure teachers leave the GenCyber camp with two lesson plans that can be implemented upon their return to their classrooms.
3. All teacher program participants ***must*** reside in the United States and be a teacher or plan to become a teacher at a school in the United States.

2020 GenCyber Grant Proposal Submission Components and Deadline

Proposal submissions should include the following components: 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.

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.

It is recommended to review the proposal evaluation criteria prior to and while preparing the program narrative section of your proposal.

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. The budget can be accessed within the proposal submission site after you have registered for an account. Budget instructions are included as Appendix F within this document. Once all required information is entered into the site, budgetary information on the Proposal Cover Sheet will automatically be populated.

Proposal Structure

All submitted proposals must include the following:

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

- Budget Worksheet
- Supporting Budget Documentation (i.e., quotes, payroll information)
- Signed Application for Federal Assistance - SF424
- Budget Information – Non-Construction Programs - SF424
- Signed Assurances – Non-Construction Programs - SF424B
- Signed Certification Regarding Lobbying Form
- If lobbying is occurring, Disclosure of Lobbying Activity – SF LLL
- Audit Report A-133 – (if you have a link/URL where report is posted, provide only the link. Otherwise, upload the document.)
- Certificate of Liability Insurance

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

Proposal Narrative Format

1. 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.
2. Page Setup Parameters:
   A. Paper Size, Width – 8.5”
   B. Paper Size, Height – 11”
   C. Margins (Top, Bottom, Left, Right) – 1”
   D. Gutter – 0”
   E. From Edge (Header, Footer) – 0.5”

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.

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 October 25, 2019, in order to be considered for a 2020 GenCyber Grant.**

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

2020 GenCyber Grant Proposal Evaluation Criteria

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

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.

The Government will award to the offerors whose proposal offers the **best value** in terms of the quality of the program, 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. The evaluation will be based on a complete assessment of the offeror’s proposal.

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 2020 grant award.

Determining how well the offeror’s proposal meets the solicitation requirements will be accomplished in the following steps.

1. A determination will be made if the offeror’s proposal meets the solicitation eligibility requirements.

2. Discriminators will be identified for the proposals reflecting the unique strengths, weaknesses, significant weaknesses, and deficiencies of each offer as it relates to the criteria factors stated below.
3. The discriminators will be totaled to determine an overall technical rating.
4. The overall technical rating will be evaluated alongside the pricing for a best value determination.

The GenCyber Program Team will evaluate the offeror's total proposal for completing the program requirements as outlined in the Call for Proposals to identify strengths, weaknesses, or deficiencies of factors 1 through 3. The staff will use these ratings to assign an adjectival rating to offeror's proposals in accordance with the evaluation procedures, criteria, and ratings.

The GenCyber Program Team 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.

Factor 1: Student and Teacher Programs

1. The program is likely to attract a sufficient number of targeted participants.
2. The program demonstrates a competitive cost-per-participant in view of the proposed program type and expected outcomes.
3. The program will be offered in a safe environment for students in elementary, middle, and/or high school, as appropriate.
4. The program director will be on site for the entire duration of the camp for consultation and oversight.
5. The K-12 pedagogical expert should be on-site for the entire duration of the camp.
6. Offeror demonstrates the ability to meet all minimum personnel staffing requirements and provide suitable instructor/student ratio based upon factors such as: activities, participant age level and environment.
7. Instructors are proficient in the cybersecurity field.
8. The program aims to serve a diverse population in terms of ethnicity, race, gender, special needs, socio-economic status, and geographic location.
9. Offerors must demonstrate the capability to offer age-appropriate curriculum for a learner-centered classroom.
10. The curriculum foundation includes cybersecurity ethics, online safety, the

GenCyber Cybersecurity First Principles and/or Concepts. The curriculum outlines clear measurable learning outcomes that are age appropriate, offered in a learner-centered classroom and advance the goals of the GenCyber program.

11. The program offers a daily camp schedule including collaborative hands-on exercises for participants to apply newly gained knowledge.
12. Has a clear plan for assessing student-learning outcomes based on stated goals.
13. The program offers opportunities for participants to continue their progress after the summer experience (i.e., follow-up activities, on-line meetings, etc.).

Factor 2: Student Programs Only

1. Addresses the needs, multiple backgrounds, and learning styles of diverse learners.
2. Specifies the range of age, varied levels of cybersecurity proficiency, and diverse populations as needed (e.g., Special Education, Gifted and Talented participants, novice learners, or advanced learners).
3. Will have a qualified staff that includes experience in teaching elementary, middle and/or high school education, as appropriate to the grade level of the participants.
4. The program has a clear plan to include instructors in the preparation and delivery of curriculum and performance-based assessments.

Factor 3: Teacher Programs Only

1. Offerors must be able to demonstrate the ability to train teachers in the GenCyber First Principles and/or Concepts.
2. A clear identification of the content areas that will assist teachers with the preparation of lessons designed for teaching cybersecurity.
3. Provides for observation and/or practicum experience for participants.
4. Offerors must be able to demonstrate how they will prepare teacher participants with cybersecurity knowledge and skills in order for participants to return to their schools and generate interest through teaching and using cybersecurity concepts and practices.
5. Provides follow-up opportunities or continued support for teachers throughout the school year.

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 are carefully reviewed by a team of Subject Matter Experts consisting of an assessment team of individuals with K-12 pedagogy and cybersecurity expertise in the particular programs represented by the proposal. Care is taken to ensure that reviewers have no conflicts of interest with the proposal. The Assessment team will make recommendations for award. The Government conducts an evaluation of all eligible proposals and will make final selections.

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, bi-laterally signed grant award from the Maryland Procurement Office.

Award Conditions

The National Security Agency's award consists of:

1. The award notice, which includes any special provisions applicable to the award and any numbered amendments thereto;
2. 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);
3. The proposal referenced in the award notice;
4. The applicable award conditions, such as Grant General Terms and Conditions; and
5. Any announcement or other National Security Agency issuance that may be incorporated by reference in the award notice.

Other Information

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

Post-Grant Award Requirements

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.

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

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

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

      2) 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.

      3) 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.

      4) 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 should be routed.

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

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

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

E. 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).

F. Tangible Personal Property Report Annual Report SF-428-A

G. Tangible Personal Property Report Supplemental Sheet SF-428S

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

I. Tangible Personal Property Report Disposition Request/Report SF-428-C (Property forms may be found at: https://www.whitehouse.gov/omb/grants_forms)

2. The following deliverables ***are required*** as a condition of grant awards:

   A. Camp Final Reports (required to be submitted within three weeks of camp completion date; additional guidance will be provided in the Program Director's Guide).

   B. Surveys (required to be completed as requested throughout the grant award period).

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

      1. 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.

      2. 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.

      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.

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 other 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

Section I:

1. Program Overview
2. Implementation

Section II:

1. Target Participation
2. Recruitment
3. Enrollment

Section III:

1. Learning
2. Assessment – Conduct Performance-Based Assessments
3. Program Legacy
4. GenCyber Curricula Delivery
5. Reflection - ***Previous GenCyber Programs Only***

Section IV:

1. Program Personnel
2. Faculty Qualifications

Section V

1. Summary

Appendix B

Proposal Narrative Guidance

Statement of Program's mission that contains a series of narrative sections that allow 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 or Teacher Programs. The narrative pulls together information on the following: (1) describe who will participate in the program, (2) how will you determine goals and assessment of learning, (3) whether it will be implemented in a residential and non-residential program, (4) what resources and tools will be used, and (5) how will they help participants learn and understand GenCyber program goals?

Section I: Program Overview

1. **Program Overview:** Outline the curriculum and describe how it will address the GenCyber program goals, cybersecurity ethics, and GenCyber cybersecurity first principles and/or concepts. (When creating a student program, it is a requirement to have a K-12 pedagogical expert on the camp staff to assist with curriculum development/review/delivery.)

   A. **Teacher Programs-** Describe the opportunities participants will have to apply the new knowledge and skills they learn during the program. List opportunities for participants to continue their progress after the summer experience (follow-up activities, on-line meetings).
      - A clear identification of the content areas that will assist teachers with the preparation of curriculum designed for teaching cybersecurity.
      - Develop two cybersecurity lesson plans that are unique to the teacher's subject area.
      - Provide follow-on support structure or activities for participants (i.e. list of resources, access to google drive, etc.)
      - Provides for observation and/or practicum experience for participants.
      - Teacher Residential Programs - Please explain your rationale for offering a residential program. Describe the types of activities that will occur during evenings and weekends (if applicable).

   B. **Student Programs** - Describe the opportunities participants will have to collaborate with their peers. 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? Describe how your program will feel more like a camp versus being in school.
      - Provide a specific plan for how the program will ensure the safety and security of students when they are not involved in structured activities.

- Residential Student Program - Please explain your rationale for offering a residential program. Describe the types of activities that will occur during evenings and weekends (if applicable). Comment on the housing arrangements and the plans for adult supervision for student camps only, throughout the program.

2. GenCyber Cybersecurity First Principles & Concepts: Each GenCyber Program must specifically state which framework and corresponding first principles and/or concept(s) will be included in the curriculum. Provide a rational for the proposed framework and its relevance for the intended program participants given their ages, backgrounds, interests, etc. The proposal should demonstrate how the camp curriculum will use the selected first principles or concepts throughout the curriculum and outline how the various lessons (e.g. cryptography, Python programming, drone hacking) are unified by the chosen curriculum concept(s). The curriculum should emphasize the explicit and implied relationship among different concepts and the lessons. By making explicit connections among topics, participant are more likely to leave the program where the "whole" of what they now know is greater than the sum of the parts.

Section II: Target Participation/ Recruitment /Enrollment

1. Target Participation: Describe the student participants who you anticipate will enroll in your program. This should include information such as socio-economic status, gender, ethnicity, cybersecurity and computer knowledge/experience, grade level(s), etc., and prior GenCyber program participation. Anticipate the number of returning GenCyber campers you will accept. If you predict a high number of returning GenCyber campers, explain how you will adjust the camp schedule to this audience to ensure they are learning new and more advanced material.

2. Recruitment: Describe how you will publicize and market your program to recruit the targeted participants. How will the program attract/recruit diverse participants? GenCyber aims to serve a diverse population in terms of ethnicity, race, gender, special needs, and/or socio-economic status, and geographic location. Include a description of your retention plan to ensure that participant numbers are being met and maintained.

3. Enrollment: Justify your proposed target enrollment numbers for the year.

A. Integration of technology and hands-on experience to enhance its educational offerings.

B. Target your admissions efforts early.

C. Effective and accurate marketing campaigns to promote camps growth.

D. Pre and/or post camp professional development of leadership, faculty, and staff to teach fun and engaging relevant curriculum.

Appendix B

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

1. **Learning**: Describe the process you will use to show that each participant has met the goals of the program. The teacher uses formative assessment of student performance during the course of the lesson to adjust instruction as needed. Include examples of each instructional topic addressed by your program.

   A. Explain how the curriculum will facilitate a learner-centered classroom.
   B. Specify all content as it relates to lessons and activities and their relevance to the GenCyber cybersecurity first principles and/or concepts.
   C. 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? What methods of differentiation are used in each activity to ensure learning?
   D. How will the participants receive feedback on the evidence of learning described?
   E. How will participants be given opportunities to reflect on their learning experiences?
   F. How will you ensure that the Teacher participants will grow professionally as a result of their participation in this program?
   G. State if the curriculum is the same as your previous program? If not, what changes have been made for this proposal?

2. **Assessment:** Program outcomes are clearly defined, simply stated, and indicate the benefits for students who are reasonably capable of completing the educational camp offering. Camp learning outcomes are linked to content offered. Appropriate program outcomes clearly communicate the knowledge, skills, and abilities students will obtain upon completion of the educational offering.

   A. Describe the process you will use to show that each participant has met the goals of the program. Include examples of each instructional topic addressed by your program. Be sure that the examples you share are specific to the goals of your program.

   B. How will the participants receive feedback on the evidence of learning?

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

   D. **Teacher Programs** - How will your program address the different backgrounds and experiences that your participants bring to the program? How will you ensure that the participants will grow professionally as a result of their participation in this program?

3. **Program Legacy:** Describe the connections you established in your community (if any) as a result of the GenCyber program to grow interest among parents and local schools' systems in continued cybersecurity education at the local level program. Describe how the program will foster continued cybersecurity awareness in the community.

   A. Teacher Programs provide a clear identification of the content areas that will assist teachers with the preparation of lessons designed for teaching cybersecurity. How does your program help teachers become GenCyber leaders through applied, practical, or project- oriented research that is focused on the application of knowledge? Provide for observation and/or practicum experience for participants.

   B. Provide opportunities for student and teacher participants to continue their progress after the summer experience (follow-up activities, on-line meetings).

4. **GenCyber Curricula Delivery:** All curricula and instructional materials are appropriately designed and presented for GenCyber age appropriate education. Student opportunities for peer collaboration using materials sufficiently supports the curriculum and are delivered using readily available, reliable technology. Examples of reliable technology used to augment the GenCyber Goals:

   A. Raspberry Pi's

   B. Sphero Robots

   C. Flash Drives – loaded with software and/or the activities.

5. **Reflection of Previous 2019 GenCyber Programs Only.** List the challenges and recommendations provided in your 2019 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 IV: 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 all required to have a K-12 pedagogical expert on the camp staff to assist with curriculum development/ review/delivery.)

   A. Demonstrating the cybersecurity expertise/experience for instructional leadership.

   B. Provide the number of camp staff that will be charged with implementing your program.

   C. Provide a breakdown of the number of staff by role that will be charged with implementing your program (i.e., Program Director, Lead Instructor, Graduate Student Assistants, etc.).

   D. Provide an overall program staff to student ratio. Include Graduate students and Assistants.

   E. Additional personnel, including Instructional Assistants, guest speakers, and presenters (if applicable).

   F. 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.

   G. Describe how you will include your instructional team in the overall camp preparation.

2. **Faculty Qualification**: 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. Will there be professional development activities for the instructional staff - pre-program, during camp and/or post camp.

Section V: Summary: Brief camp summary to include learning goals, recruitment, and the legacy of program.

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 should 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 should 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 should 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.

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 should 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.

Additionally, it is highly recommended that conversations on ethics and the ethical responsibilities of cybersecurity professionals form a foundation of all camps. Ethical conversations should occur any time a participant is "on keyboard" or engaged in learning new technical skills.

Appendix D

GenCyber 2020 Student Program Curriculum Companion Guide

This document is only a guide to help you with preparing curriculum for your camp. GenCyber provides student and teacher programs with lesson plan templates, knowing that a common template design will facilitate the sharing of units, instructional strategies, and quality materials. The common template is designed to capture best practices in curriculum, instruction, and assessment. Lesson plan templates will be made publicly available.

STAGE 1: GenCyber Student Overview

Overview

Our country's national and economic security is highly dependent upon a strong cybersecurity workforce, yet we have a shortfall of skilled cybersecurity professionals. In the current elementary, middle and high school curriculum, students have minimal exposure to cybersecurity topics. GenCyber Student camp's mission is to build a pipeline of cybersecurity professionals for the nation. The goal of promoting the study of cybersecurity and developing in students the required skills necessary to build next generation information security experts will be realized through:

1. Recruiting to camp students that may not have considered studying and working in cybersecurity.
2. Educating camp participants on GenCyber Cybersecurity First Principles and/or Concepts.

The camp will offer engaging, hands-on activities, external speakers, cybersecurity competitions and future curriculum development to offer local school to integrate in local school curriculum.

Curriculum Review Question:

- Is the length of the day reasonable in terms of program goals and appropriate to the students' age?
- Do the students spend a significant part of the day involved in a variety of activities to develop their knowledge and understanding of cybersecurity?
- Are activities designed in ways that enable students to learn and develop an understanding of: safe on-line behaviors, appropriate cybersecurity ethics, and GenCyber Cybersecurity First Principles and/or Concepts? What is the ratio of instruction to hands-on learning?

What resources and tools will be used and how will they help participants learn and understand GenCyber program goals? Does the proposal indicate specific tools and resources that will be used? Is there a clear connection between the tools and resources and the program goals?

Appendix D

STAGE 2: GenCyber Student Assessment

Assessment

Learning is a cognitive process. All learning activities will involve problem-solving, decision making, reasoning and creating. The GenCyber students will also have time to reflect, analyze and critique the how and what they are learning. The focus will be to ensure participants learn and grow through the Camp experience. The GenCyber First Principles and/or Concepts will be reinforced through interactive activities, exercises, and labs. Student achievement will be assessed by:

1. Demonstrating introductory understanding of the GenCyber first principles and/or concepts through discussions and demonstrations.

2. Applying checklists for hardening applications, systems and networks. Utilizing common security tools for troubleshooting common security issues.

3. Conducting a basic forensics examination on a sample computing system. Use of tools for network security and analysis.

4. Explaining cyber ethics and citizenship to instructors and teachers.

As consumers of the information and activities planned by the instructional staff, students are an important source of information. To determine learning outcomes, students will participate in a pre/post survey experience designed to detect changes along two critical areas of engagement.

Curriculum Review Question:

- Describe the evidence you will collect to show that each participant has met the goals of the program - Is it clear how teachers will demonstrate what they have learned?
- How will the participants receive feedback on the evidence of learning? Does the proposal indicate a system for meaningful feedback to the participants? Is it clear that the feedback is connected to the learning goals of the program?
- How will your program address the different backgrounds and experiences that your participants bring to the program? 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?
- Are the assessments realistic and meaningful for the particular group of teachers given the ages of students they are instructing?
- Is the content driven by the knowledge level, and the length of the program?

Appendix D

STAGE 3: GenCyber Students Program Implementation

Program Implementation

The GenCyber student’s daily schedule will have collaborative exercises that will provide opportunities for student to apply their newly gained knowledge. The Camp is the third residential coed GenCyber program will bring rising high school sophomores through seniors to campus for one week each. While on campus, they will be exposed to core areas of cyber, including networking, programming, and security every morning. In the afternoons, the campers will be able to build your own adventure by selecting from a number of electives available. Of this instructional time, the majority of it will be through hands on learning, exposing students to new cybersecurity concepts through doing actual activities related to the GenCyber Cybersecurity First Principles and/or Concepts.

GENCYBER STUDENTS PROGRAM OVERVIEW

Category	Topics	Example Activities
	•	•

Ethics	• What is ethics? • Why is an ethical mindset important to a cybersecurity professional? • Codes of Ethics (samples) • Ethical Dilemmas in Cybersecurity	• Develop a Camp Code of Ethics-post visibly in room-remind students prior to any invasive activity • Video on the Ethics of self-driving cars (Discussion on Ethical considerations using the “trolley problem” or similar situation) • Case Studies • Student discussions on the Top Ten Ethical Issues. • Guest Speaker: Ethical hacker
Security	2. Overview of Cybersecurity • What is security? • Why is it important? • What is the national response? • What are the basic components of security? • What are the attack models and countermeasures?	• Attack and defense demonstrations • Case studies • Hands-on experiments • Invited talks • Student presentations

	3. Principles of Cryptography This module will introduce cryptography and its applications. The following questions will be answered: • What is cryptography? • What are the key technologies? • What problems can it solve?	• Attack and defense demonstrations • Case studies • Hands-on experiments • Student presentations
	4. Online Social Networks: Threats and Solutions • What are the threats? • What are the privacy issues? • How to defend? • How to perform forensic investigation?	• Attack and defense demonstrations • Case studies • Student presentations
Cybercrimes and cyber laws	5. Cyber Bullying and Other High Tech Crimes Involving Kids • Cyber Bullying • Cyber Harassment and Text Messaging • Child Pornography • Computer Hacking • Identity Theft	• Invited talks • Creation of a PSA on topic of interest • Case studies • Submit a bill to Congress exercise

Curriculum Review Question:

Describe the typical daily schedule for a participant.

- How will this schedule provide a blend of different types of activities and learning experiences throughout the day to help participants meet the identified learning goals?
- What resources and tools will be used and how will they help participants learn and understand GenCyber program goals?
- Given your curriculum, what will the participants learn and be able to do by the end of the program? Does the curriculum clearly address the goals of the GenCyber Program?
- Does the curriculum clearly specify the GenCyber Cybersecurity First Principles and/or Concepts that will be covered? Does the curriculum clearly address how the lessons (e.g., cryptography, programming) are unified to the chosen cybersecurity first principles and/or concept(s)? Does the curriculum show explicit and implied relationships among the different first principles and/or concepts in the lessons?
- Describe the opportunities you will organize or recommend to the participants for continued learning beyond the program. Is there a plan to provide resources to the students to encourage interest and continued learning in cybersecurity after the program has ended?
- Is a plan in place to allow students to continue to learn/use cybersecurity skills/knowledge after the program ends?

Appendix E

GenCyber 2020 Teacher Program Curriculum Companion Guide

This document is only a guide to help you with preparing curriculum for your camp. GenCyber provides student and teacher programs with lesson plan templates, knowing that a common template design will facilitate the sharing of units, instructional strategies, and quality materials. The common template is designed to capture best practices in curriculum, instruction, and assessment. Lesson plan templates will be made publicly available.

STAGE 1: GenCyber Teacher Overview

Overview

GenCyber Teacher Camps will range from a one-week to one-month camps. Both non-residential and residential camps are options that will introduce basic to advanced GenCyber Cybersecurity First Principles and/or Concepts and practices to elementary school, middle school and high school teachers. The camps will be followed by professional development training and some examples are:

- Interactive webinar sessions in which topics such as future university and job opportunities for students are discussed;
- Curricular sharing opportunities;
- Cyber competition team building and student clubs activities; and
- Discussions on how to teach further technical topics.

The overall outcome of the camp will be to have a cultivated group of educators who return to their schools, secure their environment, teach and stimulate interest in their students (the next generation of university students) in learning and using the GenCyber cybersecurity first principles and concepts.

Curriculum Review Question:

- Do the teacher participants spend a significant part of the day involved in a variety of activities to develop their knowledge and understanding of cybersecurity?
- Is the content of materials reasonable in terms of program goals and appropriate to the participant's background?
- Are activities designed in ways that enable students to learn and develop an understanding on: safe on-line behaviors, appropriate cybersecurity ethics, and cybersecurity first principles and/or concepts? What is the ratio of instruction to hands-on learning?
- What resources and tools will be used and how will they help participants learn and understand the GenCyber program goals?

Does the proposal indicate specific tools and resources that will be used in the program? Is there a clear connection between the tools and resources and the program goals?

Appendix E

STAGE 2: GenCyber Teachers Assessment

Assessment

Assessing the teacher participants' learning in both formative and summative ways is encouraged. The GenCyber teacher's camp should evaluate each participant's background and experience and will tailor the hands-on labs and curricular development exercises based on their backgrounds. GenCyber teacher participants will be given a set of evaluation questions at the beginning of the camp and again at the end of the camp, and it will measure the percentage increase in learning. Each day's learning could be followed by a short quiz, which will be returned and discussed the following morning. The GenCyber participants will be engaged in curriculum development at the end of each day reflecting on what they learned that day and will spend the entire last day on developing lesson plans for their classrooms. Each GenCyber participant will receive a certificate of completion and can be offered continuing education credits.

In an effort to account for different backgrounds and experiences, the GenCyber camp will follow an evaluation plan where we will seek the participants' feedback on the overall efficiency and effectiveness of the camp with a series of questions at the end of each day. Based on the feedback, we will explore ways to change delivery of materials on the following days. These factors will help ensure that all participants will acquire new learning as a result of their participation in our GenCyber camp. These assessment procedures will help to continuously improve our pedagogical processes and understand the effectiveness of these camps.

Curriculum Review Question:

- Describe the evidence you will collect to show that each participant has met the goals of the program - Is it clear how teachers will demonstrate what they have learned?
- How will the participants receive feedback on the evidence of learning? Does the proposal indicate a system for meaningful feedback to the participants? Is it clear that the feedback is connected to the learning goals of the program?
- How will your program address the different backgrounds and experiences that your participants bring to the program? 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?
- Are the assessments realistic and meaningful for the particular group of teachers given the ages of students they are instructing?
- Is the content driven by the knowledge level and the length of the program?

Appendix E

STAGE 3: GenCyber Teacher Program Implementation

Program Implementation

The GenCyber teachers' daily schedule will have collaborative exercises that will provide opportunities for teachers to apply their newly gained knowledge. A variety of tools will be used to reinforce the GenCyber concept(s) taught in the lecture discussion session. To begin the GenCyber teacher's program, the appropriate use and settings on everyday programs like web browsers and firewalls will be discussed. Password cracking and password checking tools will be used to stress the importance of self- protection.

Videos and webinars from outside sources, TED talks, and recorded scenarios from other social media sites will be used to demonstrate problematic security issues and provide teachers with examples to use in their classes.

GENCYBER TEACHER'S PROGRAM OVERVIEW

Day 1: Fundamentals of Networks

Objectives:

- Explain protocol functionalities in the TCP/IP model.
- Explain how internetworking works.
- Explain vulnerabilities and countermeasures in network protocols. Emphasize the concept of Thinking like an Adversary in order to defend networks.

Day 2: Cryptography Fundamentals

Objectives:

- Explain the importance of number systems and operations.
- Explore common cryptographic standards.
- Describe the importance of cryptography as it applies to the confidentiality and integrity of data.

Day 3: Fundamentals of Cyber Security, Risks, and Policies

Objectives:

- Raise cyber security awareness.
- Recognize threats.
- Understand risks.
- Assess security needs

Day 4: Forensics, Ethics, and Privacy

Objectives:

- Explain the importance of computer and network forensics.
- Explain privacy issues in cyberspace.
- Explain ethical usage of cyberspace.

Day 5: Curriculum Development

Objective:

- Create lesson plans for classrooms

Curriculum Review Question:

Describe the typical daily schedule for a participant.

- How will this schedule provide a blend of different types of activities and learning experiences throughout the day to help participants meet the identified learning goals?
- What resources and tools will be used and how will they help participants learn and understand GenCyber program goals?
- Given your chosen framework, what will the participants learn and be able to do by the end of the program? Does the curriculum clearly address the goals of the GenCyber Program?
- Does the curriculum clearly specify the GenCyber cybersecurity first principles and/or concepts that will be covered? Does the curriculum clearly address how the lessons (e.g., cryptography, programming) are unified to the chosen cybersecurity first principles and/or concepts? Does the curriculum show explicit and implied relationships among different first principles and/or concepts and the lessons?
- Describe the opportunities you will organize or recommend to the participants for continued learning beyond the program. Is there a plan to provide resources to the students to encourage interest and continued learning in cybersecurity after the program has ended?
- Is a plan in place to allow students to continue to learn/use cybersecurity skills/knowledge after the program ends?

Appendix F

2020 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 should 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 one-year timeframe.

Before starting your budget, please obtain and have all supporting budget documentation for upload into the system. Supporting budget documentation should 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.) Should 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.

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

- Monetary gifts, gift cards, gift certificates and/or payments to attend camp for student participants.
- Gifted laptops 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.

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." 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 • Clerical Staff • Camp Counselor The required documentation validating salaries must be submitted in one of the following 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. *Insurance refers to additional coverage purchased specifically for the duration of the program.	• Clerical Support • Janitorial Staff • Security Staff • PKI/Token • Insurance*

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 • Non-profit organization contracted staff
Section D		
Travel	Include your estimated travel expenses pertaining to the GenCyber spring and fall meetings. Attendance is mandatory for the program director and lead instructor. 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/allowances offsetting airfare/rail for travel to a program site are only permitted for teacher programs as part of a stipend.	The spring meeting will be held in late April/early May of 2020. The fall meeting will be in mid-September 2020. Both meetings will be held in the Baltimore/Washington Metropolitan area. • Vehicle Rental • Parking • Guest Speaker Travel • Metro/Subway Fare Cards • Teacher Participant Travel Allowance as part of Stipend *Travel for professional development conferences are **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 2020 fiscal year.) Please budget for higher than normal fares for the 2020 Spring Meeting. If the grants are awarded later than anticipated, ticket prices to the Spring Meeting may be higher than anticipated as a result of last minute purchases.	
Section E	**Description**	**Example/Budget Line**
Facilities	In this category, list costs related to the rental of space for your GenCyber summer 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 • Toner

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.) 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.) The purchase of furniture is **not** allowed.	• Printers • Copy Machines • Computer Kits/Parts • iPads/Tablets *(Classroom use or Teachers Only)* • Laptops *(Classroom use or Teachers Only)* • Raspberry Pis • Arduino • Drones • Robotics • Digital Cameras
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
Section G	**Description**	**Example/Budget Line**
	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	Detail the tuition costs or mandatory fees that the grant will cover for participants. Tuition is a sum of money charged for instruction by a school, college, or university. Fees are charges that schools, colleges, or universities sometimes require. A detailed explanation is required to demonstrate that costs are not duplicated elsewhere in the budget. Teacher stipends should 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 should 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*) • Scholarships • Tuition • Continuing credits application • Mandatory University charges • Administrative processing • Evening and weekend activities • Supplies given to participants

Appendix G

Document Revision History

Version 20191002a – published October 2, 2019

- Revised Page 4, Section “GenCyber Curriculum”, second paragraph (begins “GenCyber will provide a lesson plan template…”)