CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

GenCyber & Cybersecurity Camp Proposal Toolkit

Sample language that can be deployed in GenCyber's proposal process and adapted for other cybersecurity camp proposals that request the inclusion of cybersecurity curriculum

CYBER.ORG Proposal Toolkit

Copyright © 2020 Cyber Innovation Center

Letter of Support

[Name]
[Street address]
[City, state, zip]
[Date]

[Recipient Name]
[Title]
[Organization Name]
[Street Address]
[City, state, zip]

Dear **[recipient name]**,

This letter is being written in support of the proposal being developed by **[XX]** for a new GenCyber camp opportunity. The NSA's GenCyber program is ideally designed to reach thousands of school age students and prepare them to become the cyber workers for the next generation. By partnering with this proposal, CYBER.ORG is supporting one of the more forward-looking opportunities as they seek to impact a unique population of students in the **[XX]** region.

Cybersecurity labor market surveys predict a major national cybersecurity workforce shortage. According to CyberSeek, there is a current national workforce of more than 900,000 cybersecurity professionals with a shortage of more than 500,000. The Bureau of Labor Statistics indicates Information Security Professionals to be among the 20 fastest growing occupations. The expected growth between 2019 and 2029 is 31%; that is much faster than average workforce growth.

Through the GenCyber program, students will learn about the opportunities and threats that exist in their cyber world and how they can begin to develop the skills required to succeed in cybersecurity at both the state and national levels in their future careers. The program will align with GenCyber key principles and concepts, so students will be learning about relevant, real world issues that will encourage them to pursue cybersecurity as a career option after school.

As a partner in this program, CYBER.ORG would support **[specific support language to be determined…]**

Sincerely,
[Name]

Copyright © 2020 Cyber Innovation Center

Proposal Language

CYBER.ORG will provide its curricula, provide participants access to a robust library of cyber-based curriculum and activities, and **[XX]** highly qualified members of its professional development team to lead the camp activities.

CYBER.ORG is an ongoing recipient of a Department of Homeland Security grant ($21.5M every five years) to continue its development and distribution of scalable educational materials for teaching the next-generation, cyber-literate workforce.

This GenCyber camp is designed for middle and high school teachers with moderate technology skills who possess little or no programming or cybersecurity knowledge. Camp participants will be immersed in a hands-on, experientially rich curriculum that incorporates cybersecurity ethics, safety, and GenCyber First Principles and concepts.

Follow-up professional development will include webinars, face-to-face training opportunities, and access to online resources. All teacher participants will be encouraged to participate in CYBER.ORG's teacher leader network and, as members, have access to an online resource repository, access to follow-up training, and attendance at regional cybersecurity advisory meetings and special events. The camp will incorporate a three-pronged curriculum approach that addresses GenCyber Principles and Concepts. Participants will engage with content from two CYBER.ORG courses: Cybersecurity and Cyber Society, which seamlessly work together to address the principles and concepts. Additionally, teacher participants will develop lesson plans that will help them translate the material learned during the week directly into learning experiences for students.

Cybersecurity Course

From CYBER.ORG's Cybersecurity course, teachers will work with a live cyber range that will allow teachers and students to experiment with network devices and experience how malicious attacks can affect devices, as well as allowing them to explore networks, network and system security, and data transfer. Topics discussed will include the components of a network, what it means to protect data at rest and data in transit, how passwords are protected with hash algorithms and how they can be cracked with freely available software. These discussions will be aimed at addressing each of the GenCyber principles: Data Hiding, Abstraction, Resource Encapsulation, Modularity, Layering, Least Privilege, Domain Separation, Process Isolation, Simplicity, and Minimization.

Cyber Society Course

From CYBER.ORG's Cyber Society course, teachers will work through a variety of cyber-themed scenarios to solve a series of global crises. Scenarios reflect current issues that spark deep debates about ethics, social responsibility, and values such as right to privacy, right to know and security. For example, teachers may be charged with finding the suspects behind an international hotel lockdown that was poised to host a series of international peace treaty discussions; camp participants may then need to find who was behind a Chicago bridge opening that occurred during a protest march that caused the injury and death of protesters; or they may need to investigate why a series of confidential documents are appearing in major news publications across the country. Participants will be immersed in a whole environment in the form of fictitious news articles, government briefings, and supplemental information that has been created from scratch to build the world that contains the scenario. Participants will work in small groups to think critically and work collaboratively as they pore over documents that contain not just scenario information, but significant white noise designed to confuse the many issues being discussed. These scenarios will be aimed at discussing each of the GenCyber concepts: Defense in Depth, Confidentiality, Integrity, Availability, Think Like an Adversary, and Keep it Simple.

Copyright © 2020 Cyber Innovation Center

Planning and Professional Development

Planning time will also be an integral part of the week's training agenda so that teachers have time to develop lesson plans and activities that build awareness and spark interest in cybersecurity for students. Additional camp agenda items include activities that teach and reinforce real-world life skills such as collaboration, effective communication, problem-solving, and critical thinking skills that are important in the cybersecurity field. These lessons and activities, appropriate for middle and high school students, become supplemental activities that plug and play into all content areas and will be available online at the CYBER.ORG and **[XX]** websites. Presentations of teacher created lesson plans will occur on Day 5 and these teacher-created resources will be posted on a repository hosted by **[XX]** and made available to teachers throughout the region.

High quality professional development goes beyond the 'one and done' approach where teachers are exposed to concepts in a one-time workshop and instead requires a fundamental change in the teacher's practice that will positively impact student learning. **[XX]** and CYBER.ORG both provide high quality professional development and through the camp design have developed a plan that provides for the following:

- Professional development delivered in context with the teacher's subject area (middle and high school teachers from all disciplines are the intended audience)
- Professional development occurs over time and is on-going using a structured Network that includes on-going training and support
- Flexible groupings to accommodate varying readiness levels
- Leadership opportunities for teachers with more advanced skill sets
- Train the Trainer model to develop a cadre of teachers who can provide cybersecurity training at district and site locations throughout the region

The topic of cybersecurity will be highlighted in conversations throughout the week-long experience. From the cyber range environment in Cybersecurity to the scenario analyses in Cyber Society, cybersecurity will be an overarching theme of the week.

Live Cyber Range

During the live cyber range activities in Cybersecurity, participants will be considering the strength of passwords that they may be using to secure their data. The realization that password cracking tools are readily available to anyone who wants to use them, either for good or for bad, can be an enlightening conversation, conversations will drive towards topics of resource encapsulation, layering, and least privilege. Additionally, when identifying routes that data take during transit from device to device, participants will be encouraged to consider the access points to their data at each stop in the route. During a traceroute, one can see the individual hops that a packet of data takes but how does one know if that hop is a legitimate device? What's to say that a particular device isn't being monitored by someone with malicious intent? If so, is the data that is traversing the network protected? Will it arrive intact? Will it get to the intended participant? These are all questions that must be asked when considering the impact of the entirety of the CIA triad of cybersecurity – confidentiality, integrity, and availability. Other conversations that will be modeled for participants in this session will include topics on data hiding, abstraction, domain separation, process isolation, simplicity, and minimization.

Copyright © 2020 Cyber Innovation Center

Throughout the Cyber Society scenarios, participants will engage in a variety of team building and collaboration activities. By presenting the team with a multitude of documents all at once with a limited amount of time to process them, they will be left to delegate tasks and identify roles among themselves. It is always interesting to watch how different teams approach the task. Throughout the scenario analysis activities, participants are engaged in a series of conversations with the intent of revealing content connections to the concepts of defense in depth, confidentiality, integrity, availability, think like an adversary, and keep it simple.

A Learning Experience for the Classroom

Throughout the week-long experience, teachers will be led through a learning experience that allows them to see the content as it might be delivered in a classroom. The CYBER.ORG model of professional development gives teachers the opportunity to see the content from a student's perspective. Teachers are introduced to the workshop team and from there on, are led through the content as if they were students. The workshop team uses presentation files directly from the curriculum, handouts from the curriculum, and discussion questions are presented exactly as they are intended to be delivered to students. For what it's worth, not all of the questions in the content have direct answers. But for this particular activity, teachers will be shown how fruitful the discussions can get if multiple traceroutes are run and the results are sketched on a whiteboard. For example, while the traceroute in the provided example was run to TPIC, a Turkish petroleum company, traceroutes can also be run to the BBC or to other international destinations. Should we be concerned about the security and integrity of data passing through these locations?

Copyright © 2020 Cyber Innovation Center