Statement for the Record of Kevin Nolten, Director of Academic Outreach, CYBER.ORG

Before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection & Innovation

On "The Cyber Talent Pipeline: Educating a Workforce to Match Today's Threats"

Thursday July 29, 2021 10:00 AM

Good morning, Chair Clarke, Ranking Member Garbarino, and distinguished Members of the House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection & Innovation. Thank you for the opportunity to testify before you today. I am Kevin Nolten, Director of CYBER.ORG, the academic initiative of the Cyber Innovation Center, headquartered in Bossier City, LA.

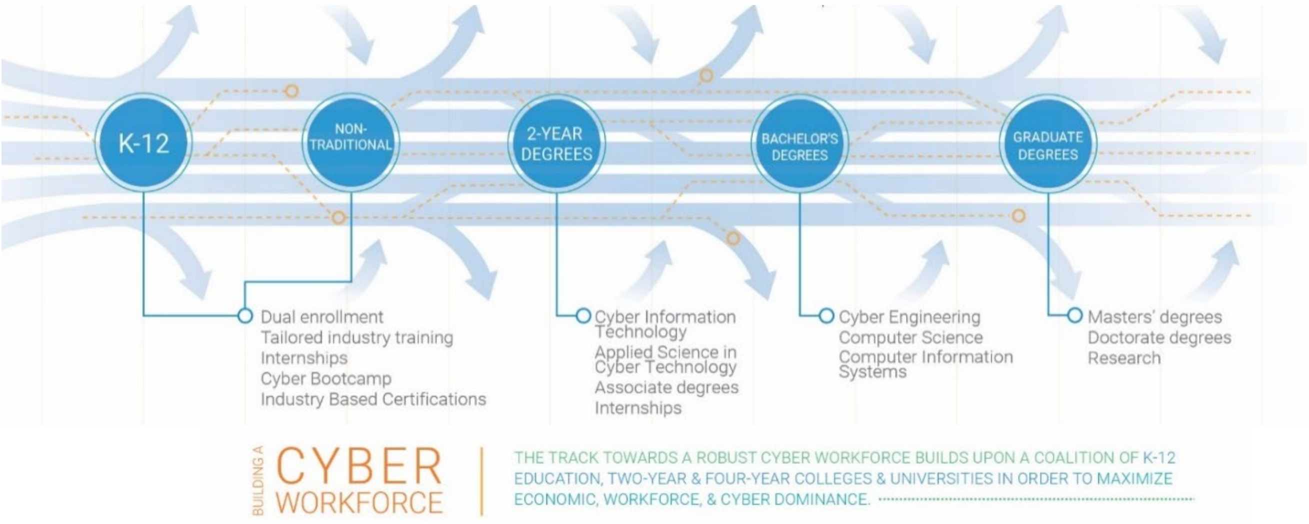
CYBER.ORG is an initiative focused on cybersecurity workforce education and development. CYBER.ORG is appreciative of the support we receive from a grant from the Department of Homeland Security's (DHS) Cybersecurity Infrastructure and Security Agency (CISA) as the lead performer of the Cybersecurity Education Training Assistance Program (CETAP) program.

I commend this subcommittee for seeking to address the longstanding challenges facing cyber workforce development efforts, specifically as they relate to K-12 cybersecurity education and preparing the next generation for the jobs of tomorrow. My testimony will address the role K-12 cybersecurity education plays in creating a foundation of future cyber workers by closing the cybersecurity skills gap and supercharging the future cybersecurity workforce for DHS and industry.

I would first like to provide the subcommittee with a brief overview of my background in education and the origin of CYBER.ORG. Prior to joining CYBER.ORG, I was an educator and school administrator, which provided me with a unique perspective on the education system and the critically important role educators play in providing students with the skills they need to succeed. This ignited my lifelong passion for educating students, helping them prepare for their futures and ultimately improving K-12 education nationwide. In my role at CYBER.ORG, I direct the organization's programmatic outreach efforts and partnerships with the goal of increasing students' access to K-12 cybersecurity curriculum. At CYBER.ORG, we approach the cybersecurity workforce gap as a national competitiveness issue and believe that increasing cybersecurity literacy will improve U.S. economic and national security. Providing students with an educational foundation and career awareness is imperative to advancing the U.S. cybersecurity workforce.

ABOUT CYBER.ORG

CYBER.ORG is the academic initiative of the Cyber Innovation Center (CIC), an economic development and technology innovation organization focused on growing the regional economy and supporting the national security enterprise through collaboration in mission-critical areas, such as the cybersecurity of our nuclear command, control, and communications systems. The CIC was founded in 2007 with the mission of diversifying the regional economy from primarily oil & gas and agriculture to include 21st-century, knowledge-based jobs in the cyber and information technology (IT) fields. The CIC recognized that to attract cyber and IT companies and jobs, the region would need a ready and able cyber workforce, and building that workforce would require a new approach to education. The success of our model has completely transformed the regional economy in northwest Louisiana: cyber and IT are now equal to the oil & gas sector in economic impact and jobs. The operational success around cybersecurity the CIC gained at its inception furthered the demand for a comprehensive workforce development program – thus the launch of CYBER.ORG, whose K12 focus represents the entry point onto the Cyber Interstate.



THE TRACK TOWARDS A ROBUST CYBER WORKFORCE BUILDS UPON A COALITION OF K-12 EDUCATION, TWO-YEAR & FOUR-YEAR COLLEGES & UNIVERSITIES IN ORDER TO MAXIMIZE ECONOMIC, WORKFORCE, & CYBER DOMINANCE.

Created in 2011, CYBER.ORG (formerly the National Integrated Cyber Education Research Center or NICERC) identified a specific need in K-12 education for a systematic and integrated solution that would build the foundation for educating the next-generation, cyber-literate workforce. Our goal was to engage K-12 students in STEM, computer science and most importantly, cybersecurity. Since then, we have implemented an integrated curricular experience across multiple academic disciplines through the development of project-driven, hands-on curricula; delivered educator professional development; established K-12 cybersecurity-based pathways; and created national cybersecurity competitions; and.

CYBER.ORG was initially created using state and local funds but was identified by the Department of Homeland Security in 2011 as an exemplar program and received funding to scale its efforts across the country. As a result of this funding and support, over the last eight years CYBER.ORG has built a K-12 cyber education program with age-appropriate content that aligns with individual state standards for education. The impact of that work is measured in thousands of teachers and millions of students with access to more content, resources and training that will fuel the cyber workforce pipeline for the future.

THE CHALLENGE

The U.S. has been struggling to solve the cyber workforce shortage in this country for too long. The workforce gap that exists today is directly connected to the country's lack of attention to STEM (science, technology, engineering, mathematics) education 15-20 years ago. Very similar to the Space Race, the United States must ensure that our students, the future workforce of our country, are equipped with the knowledge, skills, and abilities to defend against vulnerabilities in cyberspace.

CYBER.ORG recognizes this mounting challenge and has built a successful educational model that is critical to ensuring that teachers can teach cybersecurity and students have the skills necessary to meet future workforce needs. The recent, unprecedented cyberattacks like the SolarWinds and Colonial Pipeline clearly demonstrate the adverse effects of our national cybersecurity vulnerabilities, which can in part be attributed to the U.S. workforce shortage. We must increase resources and partnerships with real investments in our future U.S. workforce to ensure we are better equipped to deal with emerging technological threats.

Statistics highlight the urgency of this challenge, as increasingly complex attacks are occurring at a time when there are more than 464,000 unfilled cybersecurity roles in the United States. Filling these positions is essential to protecting both public and private organizations from outside threats, advancing U.S. innovation, and diversifying our country's cybersecurity workforce. The first step toward doing this is educating students on cybersecurity literacy as early as kindergarten.

CYBER.ORG APPROACH - EMPOWER EDUCATORS TO PREPARE THE NEXT GENERATION CYBER WORKFORCE

Advancing the cybersecurity workforce is critical to protecting the country's national security and advancing its cybersecurity posture. K-12 cybersecurity education plays a fundamental role in helping students develop the skills needed to pursue cybersecurity careers in greater numbers. As such, the CETAP Program is crucial to providing the United States with the professional level expertise needed to solve the cyber challenges of tomorrow, but more can be done to support these efforts. CYBER.ORG has developed a multi-pronged approach to ensuring students nationwide have the educational cybersecurity foundation and career awareness needed to advance the national cybersecurity workforce.

QUALITY CURRICULUM AND EFFECTIVE PROFESSIONAL DEVELOPMENT

Through CETAP, CYBER.ORG develops and distributes cyber and cybersecurity curricula to K-12 educators across the country at no cost to the educators. The CYBER.ORG approach supports cybersecurity curriculum development to provide resources for elementary and secondary school teachers that foster foundational cybersecurity awareness, cybersecurity career awareness, and technical cybersecurity skills. The curriculum is mapped to relevant state and national standards and includes resources that make up 20+ full years of curriculum (180+ hours). The curriculum is developed by subject matter experts in K-12 education, including faculty from higher education institutions across the country and representatives from industry and government. The CYBER.ORG team, who serve as lead developers, are all experienced educators, many carrying a master's and/or doctorate degree in curriculum and instruction, educational leadership, and educational technology.

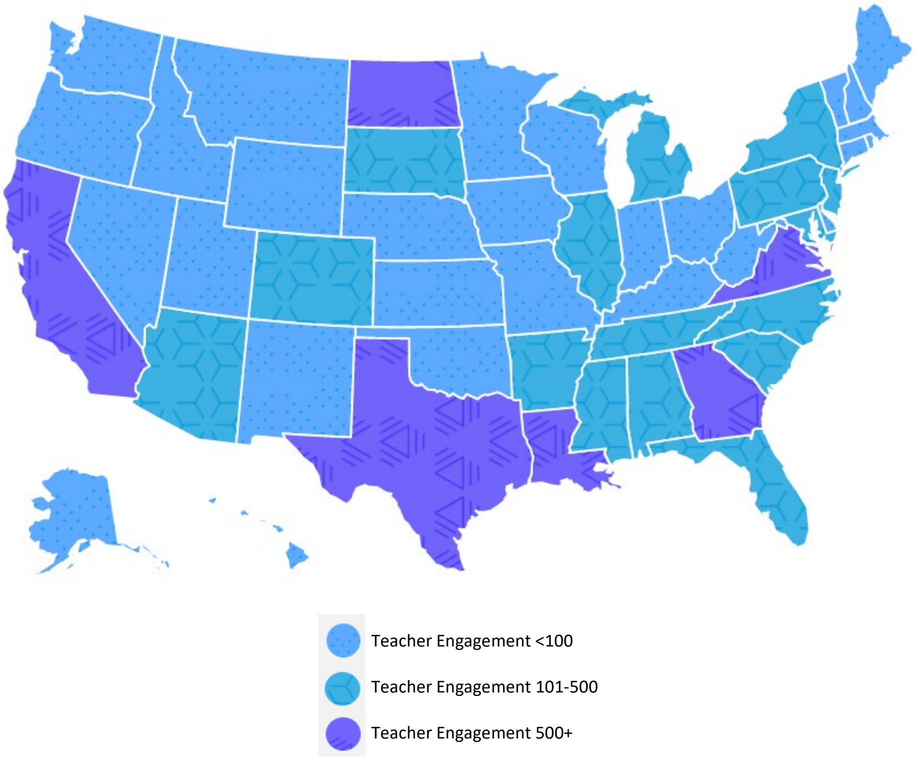
CYBER.ORG currently provides K-12 cybersecurity workforce development assistance to educators in all 50 states, with a cumulative estimated impact of over 3,000,000 students. More than 23,000 teachers are currently enrolled in CYBER.ORG's content platform and over 17,000 teachers have been trained to use CYBER.ORG content for K-12 cybersecurity education.

CYBER.ORG, in August of 2021, will publish the country's first set of national K-12 cybersecurity learning standards. Currently, there are only a few models of state-developed cybersecurity standards and no national standards specific to cybersecurity. The goal with the standards is to increased access to cybersecurity education opportunities for students that will prepare them to enter the workforce or to expand their study in college. The standards will take two approaches. The first is ensuring students have a foundational cyber understanding and knowledge to live, work, and play in cyberspace safely. The second is ensuring students have the technical skills to pursue industry-based certifications such as CompTIA's IT Fundamentals, A+ and Security+.

NATION-WIDE DEPLOYMENT

Over the past eight years, CYBER.ORG has been the lead technical institution for CETAP as it has developed and distributed a scalable program for educating the next-generation, cyber-literate workforce through a replicable educational solution for state departments of education, school districts, and individual educators from across the county.

CYBER.ORG has made a significant impact in advancing K-12 cybersecurity education in states across the country thanks to partnerships with government, educators, and school districts. With both a top-down and bottom-up approach, CYBER.ORG has been able to not only align programs to relevant state standards, help states develop cyber-related standards and pathways, and scale programming throughout the country, but also has been able to provide classroom-specific resources to educators wishing to implement modules on ransomware, or other cybersecurity topics.



https://cyber.org/about-us/our-impact

In addition to partnering with state departments of education, school districts, and classroom teachers, CYBER.ORG also prides itself on engagement with community organizations, non-profits, and industry. For example, in partnership with Palo Alto Networks, CYBER.ORG worked with the Girl Scouts USA to develop 18 cybersecurity badges to introduce more young women to cybersecurity. To date, more than 200,000 cybersecurity badges have been earned by Girl Scouts from across the country.

CYBER.ORG is also working with another global cybersecurity defense contractor to develop a 'badging' program to ensure K-12 students have skill sets and industry-based certifications to pursue 2- and 4- year degrees or jump straight into the cybersecurity workforce immediately after high school.

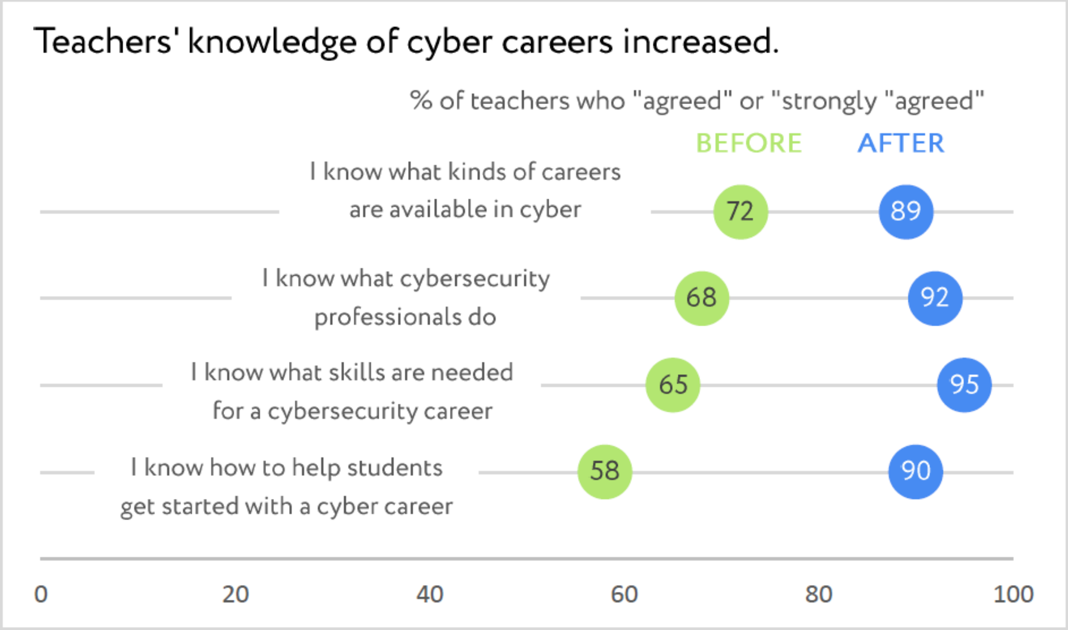
In the national delivery, CYBER.ORG has seen 64% of the teachers trained over the past 3 years come from Title 1 schools, that is schools that service students from low socioeconomic communities. Additionally, the efforts around diversifying the cybersecurity workforce have been very deliberate. Recently, CYBER.ORG launched a K-12 Historically Black College and University (HBCU) and Minority Serving Institution (MSI) Feeder Program to further strengthen the talent pipeline and increase the number of minority students pursuing cybersecurity degrees. CYBER.ORG is in the process of developing a K-12 feeder program for Grambling State University (GSU), a HBCU and the first university in Louisiana to create a cybersecurity undergraduate degree. In 2021-2022, CYBER.ORG will replicate this program between minority-serving school districts and HBCUs across the country.

The current reach of the CYBER.ORG curriculum content has impacted student achievement and interest in STEM and cyber career pathways. In a 2021 evaluation conducted by CYBER.ORG, 66% of students who completed CYBER.ORG's Cybersecurity course wanted to explore career options in cybersecurity, while 48% of students intended to earn at least one cyber-related industry-based certification before graduating from high school.

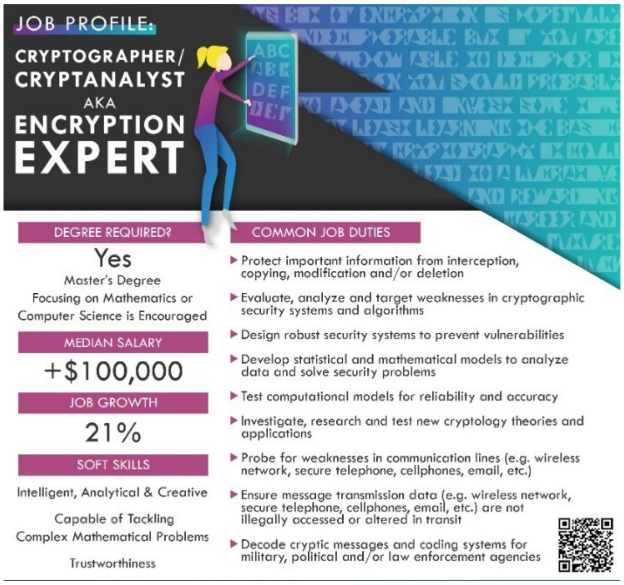
CONNECTING STUDENTS TO CYBERSECURITY DEGREES AND CAREERS

Many studies show that the formative years for a student's career trajectory occur around the middle school level, 6th-8th grade. This period, and the years leading up it, is critical for policymakers, industry, government, and educators to begin introducing students to 21st-century options – jobs that many students don't know about, and in some cases jobs that do not yet exist.

CYBER.ORG, as a workforce development organization, ensures teachers have the resources and confidence to prepare students for the next level – whether that is a 2- or 4-year college/university degree, or whether that is direct entry from high school into a cybersecurity career. This confidence is gained through the no-cost professional development offered by the CYBER.ORG team.



In addition to increasing teacher's confidence in introducing their students to cybersecurity careers, CYBER.ORG provides students with Career Profile Cards (https://cyber.org/career-exploration/cyber-career-profiles) that introduces them to jobs in cybersecurity. Aligned to the NICE cybersecurity workforce framework, each Career Profile Card teaches students about the job, the skills sets required, the degree (if any) and the certifications (if any) needed for entry into this career.



JOB PROFILE:

CRYPTOGRAPHER/
CRYPTANALYST
AKA
ENCRYPTION
EXPERT

DEGREE REQUIRED?

Yes
Master's Degree
Focusing on Mathematics or Computer Science is Encouraged

MEDIAN SALARY

+$100,000

JOB GROWTH

21%

SOFT SKILLS

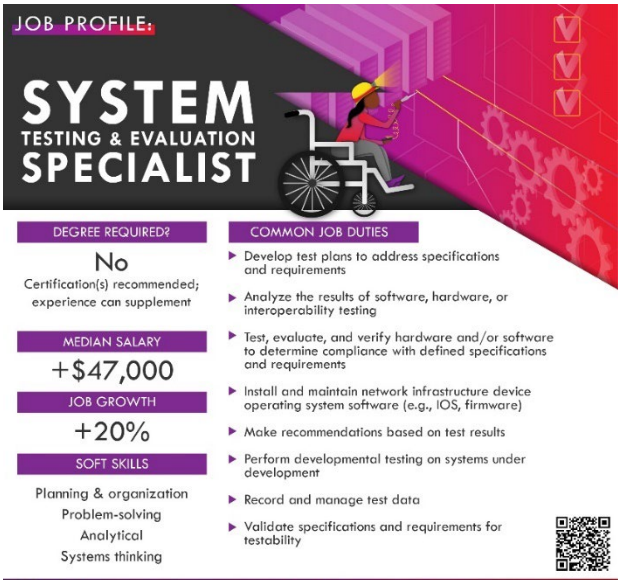
Intelligent, Analytical & Creative

Capable of Tackling Complex Mathematical Problems

Trustworthiness

COMMON JOB DUTIES

- Protect important information from interception, copying, modification and/or deletion
- Evaluate, analyze and target weaknesses in cryptographic security systems and algorithms
- Design robust security systems to prevent vulnerabilities
- Develop statistical and mathematical models to analyze data and solve security problems
- Test computational models for reliability and accuracy
- Investigate, research and test new cryptology theories and applications
- Probe for weaknesses in communication lines (e.g. wireless network, secure telephone, cellphones, email, etc.)
- Ensure message transmission data (e.g. wireless network, secure telephone, cellphones, email, etc.) are not illegally accessed or altered in transit
- Decode cryptic messages and coding systems for military, political and/or law enforcement agencies



JOB PROFILE:

SYSTEM
TESTING & EVALUATION
SPECIALIST

DEGREE REQUIRED?

No
Certification(s) recommended; experience can supplement

MEDIAN SALARY

+$47,000

JOB GROWTH

+20%

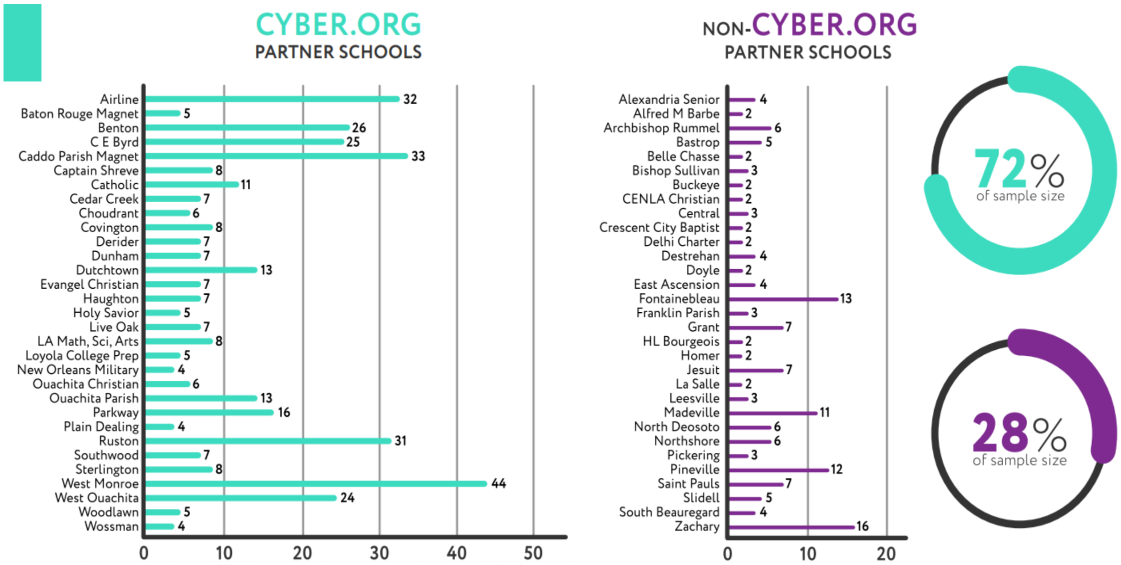
SOFT SKILLS

Planning & organization
Problem-solving
Analytical
Systems thinking

COMMON JOB DUTIES

- Develop test plans to address specifications and requirements
- Analyze the results of software, hardware, or interoperability testing
- Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements
- Install and maintain network infrastructure device operating system software (e.g., IOS, firmware)
- Make recommendations based on test results
- Perform developmental testing on systems under development
- Record and manage test data
- Validate specifications and requirements for testability

The multi-faceted approach CYBER.ORG takes yields results. A regional study (https://cyber.org/sites/default/files/2020-06/Louisiana%20Study.pdf) found that high schools with teachers enrolled in CYBER.ORG curricula on average sent, in total, ***four times more students*** into cyber-related college of university degree programs as those that did not.



For the puposes of the pilot study, a CYBER.ORG partner school is defined as having at least 1 teacher with access to CYBER.ORG's curriculum library.

INVESTING IN K-12 CYBER EDUCATION

The solution for solving the cybersecurity workforce shortage is developing a capable pipeline of cybersecurity professionals who are entering the workforce at every level of education. CYBER.ORG is enabling K-12 teachers to serve as force multipliers, educating students to build the cybersecurity workforce of the future. The CETAP model and CYBER.ORG have provided a clear blueprint for bolstering the U.S. workforce pipeline for other areas critical to U.S. economic development and global technological competitiveness.

The work being done by CYBER.ORG through the CETAP program also supports the recommendations made by the Cyberspace Solarium Commission. The Commission's report on Growing a Stronger Federal Cybersecurity Workforce[1] called out the importance of the CETAP program in helping recruit the talent needed to support the federal workforce. The Solarium Commission also identified that the CETAP program has "significant room to grow." To grow, CETAP would need additional funding and resources to:

- Increased access to curricula for educators;
- Development of pathways for immediate job entry, more direct connection of high schools to post-secondary workforce pathways, and engagements with more HBCU institutions;
- Expansion of recruiting and retaining students from military families for future cyber employment;
- Development of virtual curricula, resources that can be used by schools for student asynchronous learning, particularly in rural and underserved communities; and
- Launch of a virtual cyber laboratory specifically used for K-12 educators, providing an application-based learning environment for real-world cybersecurity lessons.

Congress has recognized the importance of CETAP. With the help of this Committee's former Chair Cedric Richmond as well as Senators Rosen and Cassidy, the FY21 National Defense Authorization Act (NDAA) formally authorized CETAP and codified the program's mission as a leader in the dissemination of cybersecurity-focused K-12 education resources and training. The FY 2021 authorization was paired with an appropriation of the annual base amount of $4.3 million with an

[1] https://www.solarium.gov/public-communications/workforce-white-paper

additional discretionary funding of $1.7 million for K-12 education at CISA. With the additional funding, CETAP utilized the additional $1.7 million provided in discretionary support to enable the launch of three K-12 initiatives focusing on Historically Black Colleges and University (HBCU) feeder high schools and students with disabilities.

RECOMMENDATIONS

CYBER.ORG, through CETAP, has made a tremendous impact in states and districts across the country, but it is time to scale. Providing stable, continuous funding and legislative support for CETAP will enable the program to reach its short- and long-term goals of expanding programming in all 50 states so that every student in the United States is cyber literate and has the skills needed to pursue cybersecurity careers in greater numbers and fortify the workforce needed to combat increasingly complex attacks. The following recommendations and actions are important to large-scale impact of CYBER.ORG and CETAP.

- First, we recommend increased and sustained funding for cybersecurity education and workforce development. It is critical that CISA include funding in its annual budget request to sustain and expand the reach of the CETAP program in classrooms across the country. CETAP's cost-effective approach will get proven successful curriculum into the hands of more teachers who will continue to develop a strong, equitable pipeline of cybersecurity talent.
- Second, CETAP should be formally recognized as the K-12 feeder program for other, federal cybersecurity workforce programs. Connecting students directly to programs such as Centers for Academic Excellence, Scholarship for Service, Federal Apprenticeship Program, and others will ensure these federal efforts complement one another and provide the best workforce outcomes possible.
- Third, we recommend special attention be given to “what’s next” after the different academic milestones (K-12, higher education, reskilling, etc.) - that is, addressing the need for connecting students to cybersecurity jobs. Importantly, connecting students, whether high school, college, university graduates, or non-traditional students to the cybersecurity workforce is a critical step in closing the workforce gap in the country.

CONCLUSION

It has been an honor to appear before this distinguished panel of policymakers. Thank you, Chair Clarke, and Ranking Member Garbarino for your dedication to growing and advancing the cybersecurity workforce.

K-12 cybersecurity education must be viewed as the vehicle in which we can introduce the next generation of cybersecurity professionals to careers in the field. Expanding K-12 cybersecurity education is critical to addressing the cybersecurity workforce shortage. DHS has created a proven, cost-efficient model to train educators in cybersecurity and reach more K-12 students in classrooms across the country with cybersecurity curriculum. The CETAP program requires additional investment to close the cybersecurity workforce gap and grow the cybersecurity skills pipeline.

CYBER.ORG envisions a future where every student is cyber literate and has the option to pursue cybersecurity careers. We look forward to working with the Committee and serving as a resource as it develops policies to advance K-12 cybersecurity. We also remain committed to working with Committee members in their states and districts to advance the CETAP program and expand access to K-12 cybersecurity education.

CYBER.ORG appreciates the opportunity to join in this worthy discussion and is willing to serve as a resource in the development of any cybersecurity education legislation going forward. We are thrilled to participate in today’s hearing and look forward to a long partnership where we can continue working to tackle this important issue.

Thank you, and I’ll be happy to answer any of your questions.