

# Virginia CyberCAMP 2016



*An Introduction  
To Careers In  
Cybersecurity  
for Students  
and Teachers*

Virginia Department of Education  
Office of Career, Technical, and Adult Education



# VIRGINIA CYBERCAMP 2016 PROGRAM

## AN INTRODUCTION TO CAREERS IN CYBERSECURITY FOR STUDENTS AND TEACHERS

**Evaluation Report**  
**Developed by the**  
**Office of Career, Technical, and Adult Education**  
Virginia Department of Education  
Richmond, Virginia

March 2017

Yvonne V. Thayer, Ed.D.  
Principal Investigator



# VIRGINIA CYBERCAMP 2016 PROGRAM

## AN INTRODUCTION TO CAREERS IN CYBERSECURITY FOR STUDENTS AND TEACHERS

The Virginia CyberCamp 2016 Program introduced students, teachers, school counselors, and school leaders to careers in cybersecurity through a 70-hour summer program conducted in school divisions in each of the eight Superintendent's Regions. This program offered instruction in basic programming skills, explored many of the career opportunities in cybersecurity, and encouraged students to earn a cybersecurity-related credential. The curriculum used to plan the program was supported with staff development that equipped the teachers to plan engaging learning experiences that would develop interest in cybersecurity careers. The Office of Career, Technical, and Adult Education at the Virginia Department of Education developed the CyberCamp Program, one of several learning opportunities that introduce high school students to career pathways in cybersecurity. This report will share the design of these camps, professional development for teachers, observations while camps were in session, outcomes related to camp goals, and directions for future activities.

## BACKGROUND

### Cybersecurity education is a state and national priority.

In February 2014, Governor Terry McAuliffe established Cyber Virginia and the Virginia Cyber Security Commission through Executive Order 8. The work of the governor and the commission raised awareness of the growing careers in cybersecurity and the continuing need to improve the educational pipeline to fill thousands of unfilled and emerging jobs in Virginia. The Office of Career, Technical, and Adult Education recognized the importance of including content, courses, and programs related to cybersecurity careers in career and technical education (CTE) programs. They developed cybersecurity infusion units of study that teachers integrated into existing technical courses. Representatives from school divisions, colleges and universities, and Virginia businesses were brought together to begin the process of developing a new cybersecurity career pathway for Virginia students.

In 2016, the Virginia Department of Education published a research report, *Virginia's 21st Century Career Pathway – Cybersecurity*, which spoke to the state's current efforts to prepare more workers for cybersecurity careers and recommended several actions that could strengthen K-12's role as the entry point into the cybersecurity education pipeline. Since the publication of the report, the CTE has worked with employers, teachers, and school leaders to develop the framework and competencies for a cybersecurity career pathway that prepares students who are interested in a variety of cyber careers – those in safety and security, business, STEM, and information technology.

At the national level, attention is being placed on cybersecurity education in the public schools. The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a nationally coordinated effort to advance education and training opportunities for cybersecurity preparation. NICE coordinates with government, academic, and industry partners to build on existing successful programs and bring leadership to increase the number of skilled cybersecurity professionals. NICE has a K-12 working group of educators who meet monthly to share the progress that schools and states are making to increase courses, career pathways, student competitions, or other cyber activities. Conferences are held to continue a conversation about adding cybersecurity education to the priorities of public education.

As cybersecurity is being discussed in the K-12 setting, NICE encourages educators to learn more about cybersecurity competitions as one way to develop skills to meet the emerging workforce needs. (See [http://csrc.nist.gov/nice/documents/cybersecurity\\_competitions.pdf](http://csrc.nist.gov/nice/documents/cybersecurity_competitions.pdf)). Local, regional, national, and international competitions engage individuals or teams in cybersecurity activities that may be a one-day event or a series of face-to-face or virtual events. A few of the well-established competitions are the cybersecurity version of Capture the Flag, the Air Force Association's CyberPatriot, and the Center for Internet Security's US Cyber Challenge.

As was noted in *Virginia's 21st Century Career Pathway – Cybersecurity*, employers view cybersecurity competitions positively because these events provide experience with authentic security activities. A recent report on cybersecurity games concludes that competitions build soft skills as well as technical skills, which are an ongoing request of cybersecurity employers (Katzcy Consulting, 2016). Laurin Buchanan, principal investigator at Secure Decisions, believes that competitions may be a proxy for apprenticeships because participants (1) experience work roles that are relevant to cybersecurity, (2) work under pressure, (3) demonstrate dedication and interest in the work, (4) practice communication skills, and (5) demonstrate collaboration and teamwork (Buchanan, 2017).

One of NICE's contributions to education is the development of a cybersecurity workforce framework that organizes cybersecurity into seven high-level categories, each comprised of several specialty areas. Based on the NICE framework, the National CyberWatch Center K-12 Division, ETPro, and the National Science Foundation published a Cybersecurity Career Wheel to assist educators, students, and parents to understand cyber-related career options and pathways. The following chart is a representation of the information in the Career Wheel. [NICE has updated the National Cybersecurity Workforce Framework, and it will be distributed in Spring 2017.]

## National Initiative for Cybersecurity Education (NICE) Workforce Framework CYBERSECURITY CAREERS

Cyber Speciality Area	Degree/Training	Classes to Take	Future Job Demand	Mean Salary Range
<b>Oversight and Development</b>	<p>ADVANCED DEGREES BUSINESS CRIMINAL JUSTICE INFORMATION TECHNOLOGY LAW</p> <p><i>Providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work</i></p>	<p>Information Technology Business Law Cyber Ethics Project Management e-Government e-Business Strategic Planning Privacy Rights and Civil Liberties Intellectual Property</p>	Medium	\$100,000+
<b>Securely Provision</b>	<p>COMPUTER SCIENCE ELECTRICAL ENGINEERING NETWORKING SYSTEMS DEVELOPER</p> <p><i>Conceptualizing, designing, and building secure IT systems</i></p>	<p>Business Engineering Math Networking Programming Languages (C++, C#, Java) Project Management</p>	High	\$89,280 - \$96,600
<b>Protect and Defend</b>	<p>COMPUTER SCIENCE CRIMINAL INVESTIGATION ENGINEERING FOREIGN LANGUAGE INFORMATION ASSURANCE IT AND SECURITY NETWORK SECURITY PSYCHOLOGY</p> <p><i>Identification, analysis, and mitigation of threats to internal IT systems or networks</i></p>	<p>Programming Operating Systems Networking Cisco Ethical Hacking Computer and Network Security Security Tools/ Open Source/ Commercial</p>	<p>Medium to High</p>	<p>Dependent on Specialization FBI GS-7 to GS-11 \$55,000 - \$120,000</p>
<b>Analyze</b>	<p>ADVANCED DEGREES COMPUTER SCIENCE CRIMINAL JUSTICE ENGINEERING FORENSICS INFORMATION TECHNOLOGY LAW MILITARY</p> <p><i>Expert review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence</i></p>	<p>Computer Science Criminal Justice Engineering Foreign Language International Affairs Math Psychology Sociology</p>	Medium	<p>Security Clearance Needed Varies with Experience and Specific Job Area \$74,872 - \$155,500</p>

<p><b>Investigate</b></p> <p><i>Investigation of cyber events and/or crimes of IT systems, networks, and digital evidence</i></p>	<p>COMPUTER SCIENCE CRIMINAL INVESTIGATION FORENSIC SCIENCE INFORMATION ASSURANCE IT AND SECURITY NETWORK SECURITY PSYCHOLOGY</p>	<p>Criminal Law Programming Operating Systems Networking Mobile Device Forensics Malware Analysis Computer and Network Security Computer Security and Investigation Certifications Database Design and SQL Programming Logic and Programming Risk Analysis Operating Systems Networking Database Recovery Systems Security Web Programming</p>	<p>Medium – High</p>	<p>Location dependent \$50,000 - \$80,000</p>
<p><b>Operate and Maintain</b></p> <p><i>Providing support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security</i></p>	<p>COMPUTER SCIENCE INFORMATION TECHNOLOGY NETWORK/COMPUTER SYSTEMS</p>	<p>Electrical and Mechanical Engineering Computer Science Programming Mathematics Physics Network Architecture Network and Software Security Radio, Wireless and Cellular Networks</p>	<p>High</p>	<p>Dependent on Specialization \$55,000 - \$87,000</p>
<p><b>Collect and Operate</b></p> <p><i>Denial and deception operations and collection of cybersecurity information that may be used to develop intelligence</i></p>	<p>ADVANCED DEGREES COMPUTER ENGINEERING COMPUTER SCIENCE ENGINEERING INFORMATION ASSURANCE IT AND SECURITY MATHEMATICS MILITARY EXPERIENCE NETWORK SECURITY PHYSICS SYSTEMS ENGINEERING</p>	<p>High Security Clearance Needed</p>	<p>Varies with Experience and Specific Job Area \$74,000 - \$105,000</p>	

(<http://csrc.nist.gov/nice/framework/>)

At the Commonwealth Conference on Cyber and Education (December 2015), Governor McAuliffe challenged community colleges across Virginia to include cybersecurity courses in their program offerings. Over the last few years, Virginia’s community colleges have expanded courses and industry certifications, and universities have increased undergraduate and graduate programs to strengthen workforce readiness for cyber careers. The following colleges and universities hold national certifications in cybersecurity programs awarded by the National Security Agency and U.S. Department of Homeland Security (National Initiative for Cybersecurity Careers and Studies, 2016).

George Mason University	Academic Excellence in Cyber Defense Education Academic Excellence in Cyber Defense Research Curriculum meets national standards
Hampton University	Academic Excellence in Cyber Defense Education
James Madison University	Academic Excellence in Cyber Defense Education Curriculum meets national standards
Lord Fairfax Community College	Academic Excellence in Cyber Defense Education – 2 Yr
Marymount University	Academic Excellence in Cyber Defense Education Curriculum meets national standards
Norfolk State University	Academic Excellence in Cyber Defense Education
Northern Virginia Community College	Academic Excellence in Cyber Defense Education – 2 Yr Curriculum meets national standards
Radford University	Academic Excellence in Cyber Defense Education
Tidewater Community College	Academic Excellence in Cyber Defense Education – 2 Yr
Virginia Tech	Academic Excellence in Cyber Defense Research

Job reports continue to show a national and world shortage of cybersecurity workers. In 2015, there were more than 600,000 high-paying tech jobs unfilled in this country (Smith, 2016). By 2019, the cybersecurity workforce is expected to rise to 6 million globally, with a projected shortfall of 1.5 million. Among 1 million openings for informational security professionals worldwide, more than 209,000 cybersecurity jobs in the United States are unfilled, and the demand for information security professionals is expected to grow by 53 percent through 2018. (Morgan, Cybersecurity Jobs Report, 2016) (Morgan, One Million Cybersecurity Job Openings in 2016, 2016). Careers in information security analysis are growing at a rate of 18 percent through 2024, and careers for software developers and programmers are expected to reflect a national increase in demand for cybersecurity, an increase in the use of mobile technology, and the implementation of electronic medical records (U.S. Bureau of Labor Statistics, 2015). Healthcare organizations are currently experiencing monthly cyber attacks. A 2016 survey of IT security personnel found that half had experienced loss or exposure of patient information in the past year (Institute, 2016).

In Virginia, jobs associated with cybersecurity remain in high demand and are expected to grow through 2020. While the number of workers in cybersecurity is expected to increase by more than 17 percent nationally, the number of persons employed in cybersecurity jobs in Virginia is expected to increase by 25 percent from 2012 through 2022. A look at job openings in April 2016 found that the three occupations with the largest number of openings were network and computer systems administrators, information security analysts, and database administrators. (Virginia Economic Development Partnership, 2016).

Just as one of the priorities of STEM initiatives is to educate girls about job opportunities in STEM fields, there are efforts to attract young women into the cyber career pipeline because only 26 percent of cyber professionals are women (LeClair, 2016). Fifty percent of college graduates are women, but only 11 percent are in cybersecurity fields (Schlesinger, 2015). Concerns about career information and recruitment are not limited to young women. Raytheon and the National Cybersecurity Alliance conducted a survey of young adults and found that U.S. millennials who have read or heard about cyberattacks within the last year nearly doubled, from 36 percent in 2015 to 64 percent this year. Yet, only 33 percent of this group have sought out cyber jobs as compared to 82 percent of millennials in the Middle East. Millennials want jobs using the skills cyber professionals use – problem solving, data analysis, and communications – yet they are not approaching this industry to use their skills and may not know enough about cybersecurity jobs in general. When asked what would increase their interest in a cybersecurity career, of all surveyed internationally, 48 percent wanted to know more about what the jobs might entail, 44 percent wanted training to determine whether they would be good at cybersecurity, and 37 percent wanted an opportunity to talk with current professionals. (Raytheon and National Cybersecurity Alliance, 2016).

The call for all students to learn coding (Paul, 2016) is important, but not enough, if the cybersecurity pipeline is going to attract women and the emerging workforce. Schools must respond to what young workers need by finding opportunities for students to learn about cyber-related jobs, meet people working in cyber careers, develop problem solving and other workforce skills, and have an opportunity to experience projects that are highly similar to real work in cyber careers.

The Virginia CyberCamp 2016 Program was developed to begin addressing these needs during the last three years of high school, when students are exploring their choices for postsecondary education and careers. This pilot program was designed to model how to integrate concepts and skills associated with cybersecurity into both academic and CTE programs. The CyberCamp initiative raises awareness among students and teachers that cybersecurity and the careers associated with it are highly relevant to the world we live in. Providing students with an opportunity to explore the broad spectrum of cyber careers is a challenge K-12 is preparing to meet.

# REQUIREMENTS

## CyberCamps offer challenged school divisions a way to introduce cybersecurity to students and teachers.

The purpose of the Virginia CyberCamp 2016 Program was to develop a cybersecurity pilot program in schools across the commonwealth that would introduce high school students and teachers to cybersecurity as a career while giving them the opportunity to learn some of the basic skills associated with cyber careers. The pilot program was designed to give school divisions a model program that could inform their plans to incorporate cybersecurity education into both academic and CTE programs.

The CyberCamp program provided the opportunity for students to interact with individuals and companies that have cybersecurity as part of their work while developing knowledge and skills that can lead to industry certifications and postsecondary education in cybersecurity. The CyberCamp Program was an important introduction to cybersecurity education for many schools in preparation for a cybersecurity career pathway for CTE programs.

**Eligible School Divisions** – During the 2015-2016 school year, Governor McAuliffe announced a \$2 million state initiative to implement the extended school year Virginia CyberCamp 2016 Program targeted to high schools in challenged school divisions – those divisions with 50 percent or more of its enrolled students eligible for free and reduced price meals. Superintendent’s Memo 293-15 was issued in December 2015, announcing the requirements for participation in the initiative. (See

[http://www.doe.virginia.gov/administrators/superintendents\\_memos/2015/293-15.shtml](http://www.doe.virginia.gov/administrators/superintendents_memos/2015/293-15.shtml))

Eligible school divisions were invited to submit a CyberCamp application that proposed instructional activities, plans for professional development of teachers and school leaders, and a budget. In February, the Office of Career, Technical, and Adult Education announced that four camps would be held in each of the eight Superintendent’s Study Groups, for a total of 32 CyberCamps. Each camp received a state-funded grant for implementation of the pilot program.

**Goals for the Program** – The following goals established a statewide design for the camps:

- Increase awareness of careers in cybersecurity among teachers and students;
- Engage students in project-driven learning; and
- Introduce students and teachers to cybersecurity-related industry credentials and provide students a foundation from which they could pursue a certification during the 2016-2017 school year.

State guidance recommended that each camp include the following as components of the CyberCamp experience:

- 1) NICERC (National Integrated Cyber Education Research Center) cyber literacy curriculum and teaching resources, approved by the U.S. Department of Homeland Security
- 2) Capacity-building activities in robotics and computer programming that introduced students to information technology, networking, and computer science
- 3) Project-driven, cross-disciplinary instruction
- 4) Daily learning experiences, team projects, and a cumulative student team presentation
- 5) Career information provided by guest speakers, field trips, and online resources
- 6) Opportunity to advance toward earning the IC3 Digital Literacy Certification

**Student Eligibility** – Students were eligible to participate in the camp if they were rising 10<sup>th</sup>, 11<sup>th</sup>-, or 12<sup>th</sup>-graders and had expressed an interest in cybersecurity careers or had started a program of study related to the cybersecurity sector. Each camp location developed an application process and chose participants based on locally developed criteria. Each camp was asked to target 25 students as a participation goal and encouraged schools to recruit females as well as males, all ethnicities represented in the school, and students with disabilities consistent with other programs in the school.

**Staffing** – The camps were required to plan instructional activities as a cross-disciplinary experience, and staffing reflected this priority. Each camp identified a school leader to serve as camp director. The team that facilitated the instructional activities included academic teachers, specifically one English, one mathematics, and one science teacher; and several CTE teachers representing engineering, technology, robotics, or public safety and security. A counselor was included on the instructional team to help coordinate career-related activities. The camp director and instructional team were selected several months prior to the camp starting date so that

<b>Virginia 2016 CyberCamps</b>	
<b>LOCATION</b>	<b>DIVISION(S) SERVED</b>
<b>T.C. Williams High School</b>	Alexandria City
<b>Virginia High School</b>	Bristol City
<b>Brunswick High School</b>	Brunswick County
<b>Crossroads Institute</b>	Carroll County Grayson County Galax City
<b>Charlottesville High School</b>	Charlottesville City
<b>Cumberland High School</b>	Cumberland County
<b>George Washington High School</b>	Danville City
<b>Northern Neck Technical Center</b>	Essex County Lancaster County Richmond County
<b>Franklin High School</b>	Franklin City
<b>James Monroe High School</b>	Fredericksburg City
<b>Halifax County High School</b>	Halifax County
<b>Harrisonburg High School</b>	Harrisonburg City
<b>Magna Vista High School</b>	Henry County
<b>Hopewell High School</b>	Hopewell City Dinwiddie County
<b>Central High School</b>	Lunenburg County
<b>Osborn High School</b>	Manassas City
<b>Manassas Park High School</b>	Manassas Park City
<b>Martinsville High School</b>	Martinsville City
<b>Park View High School</b>	Mecklenburg County
<b>Nelson County High School</b>	Nelson County
<b>Heritage High School</b>	Newport News City
<b>Governor's STEM Academy</b>	
<b>Northern Neck Technical Center</b>	Northumberland County Westmoreland County Town of Colonial Beach
<b>Luray High School</b>	Page County
<b>Petersburg High School</b>	Petersburg City
<b>Pittsylvania County Schools STEM Academy</b>	Pittsylvania County
<b>I.C. Norcom High School</b>	Portsmouth City
<b>Pulaski County CTE Center</b>	Pulaski County
<b>Franklin Military Academy</b>	Richmond City
<b>Thomas Jefferson High School</b>	Richmond City
<b>Tazewell County CTE Center</b>	Tazewell County
<b>Waynesboro High School</b>	Waynesboro City
<b>John Handley High School</b>	Winchester City

the teams could participate in professional development and have adequate time to work together to develop the camp program.

# TRAINING

## Professional development is key to CyberCamp success.

While some CTE programs have used Virginia’s cybersecurity infusion units to introduce cybersecurity concepts in established CTE program areas, and many high schools offered computer science or technology courses; however, instructional teams have had little or no experience with cybersecurity education or developing a CyberCamp experience for high school students. Seeking expertise in cyber education, CTE partnered with the academic division of the Cyber Innovation Center (CIC) in Bossier City, Louisiana, to identify a researched-based curriculum for high school students that instructional teams could use as the core curriculum for the camp. NICERC and CTE agreed to use NICERC’s Cyber Literacy curriculum resources as the foundation for the CyberCamp instructional program. Using NICERC’s curriculum provided assurance that each camp would be offering a research-based curriculum and that there would be consistency in the CyberCamp programs offered statewide.

NICERC staff had successfully trained teachers across the nation to implement this curriculum. They accepted the challenge of working with 32 teams of teachers, school counselors, and school leaders who were inexperienced with cyber education and likely would require support after their training. NICERC staff collaborated with CTE staff to provide two days of research-based training in each of the eight Superintendent’s Regions over six weeks at no cost to the commonwealth.

Two hundred ninety-six Virginia educators completed the training. The major outcome of the professional development was the readiness of team members to (1) design the camp experience to include the NICERC curriculum, (2) assign instructional responsibilities to members of the team, (3) teach cyber literacy through robotics lessons and (4) teach humanities lessons and cyber ethics.

Participants commented that they “enjoyed learning about the ins and outs of programming a robot,” they “appreciated the integration of writing and researching skills,” and the robotics training “helped stretch my ability to think, reason, and problem solve.”

NICERC instructor Dr. Chuck Gardner summarized the Virginia training experience as follows:

*“Teachers learned by doing the projects that they would be instructing their summer camp students on. NICERC’s model of professional development is based on teachers working in small groups, doing the projects and assignments that are embedded into the curriculum so that teachers leave with the confidence to present the curriculum in their classrooms.”*



## NICERC'S CYBER LITERACY CURRICULUM

NICERC's cyber curriculum is project-driven, application-based, and showcases a systems-level understanding of real-world applications of science, technology, engineering, and mathematics. Liberal arts components allow teachers to embed the curriculum across multiple disciplines as they introduce students to the career pathway that leads to becoming the next generation of cyber professionals.

Cyber Literacy builds a strong cybersecurity foundation for high school students by blending robotics, programming, electricity, and elements of liberal arts. Students learn about the opportunities, threats, responsibilities, and legal constraints associated with operating in cyberspace. As students learn the basics of programming and networking they develop critical thinking skills.

- Programming introduces students to basic coding essentials through flowcharts and simple programming languages.
- Robotics uses a Parallax Boe-Bot microcontroller as the platform for teaching robotics fundamentals. Students assemble their robots to perform various functions through the implementation of sensors and application of their programming knowledge.
- Liberal Arts illustrates real-world applications and implications of computers and the Internet in our society today. Students are challenged to intensely deliberate the historical and societal context of cyber. Discussions dive deep into critical aspects of students' futures, such as the 4th Amendment of the U.S. Constitution and issues of privacy, security, and technology.

**The NICERC curriculum is available  
to K-12 teachers at no cost ([www.NICERC.org](http://www.NICERC.org))**

## PROGRAM PLANNING

### School teams develop CyberCamp programs that include state community resources.

The instructional teams worked for several weeks prior to the beginning of the camps to plan the instructional program – identifying units of study, arranging field trips, locating speakers to visit the camp, and studying the NICERC curriculum. Camp directors purchased supplies, secured space, arranged transportation, and planned healthy meals and snacks. Teams were encouraged to use the resources of community colleges and universities with cybersecurity education programs. Local businesses were asked to participate in the camps by sharing the cybersecurity threats and employment needs in local communities. As students were recruited to participate, parents and community members learned that students who applied and were selected would be among the first students in Virginia to study cybersecurity.

The Virginia Department of Education required that camps be located on a high school campus. The school division that hosted the camp provided computers for participants to use. Grant funds supplied all materials for classroom projects, transportation, and meals so that there would be no cost to either the students or the division for participating in the pilot program. Each camp planned a minimum of 70 hours of instructional time and could configure the schedule in a variety of ways (i.e., amount of time daily, number of days per week, number of weeks, and date of camp).

The instructional program reflected project-driven learning opportunities for teams of students. These projects build both academic and career-readiness skills (e.g., working collaboratively, writing reports, and making presentations) needed to pursue industry certifications and postsecondary education for cyber-related jobs. The instructional team collaborated to create a camp experience that was balanced between teacher-led instruction and students working in teams. Teachers planned to demonstrate or lead discussions about robotics, coding, cyber issues, and ethics; students would work in teams to solve problems, develop projects, and discuss interesting cybersecurity topics.

*“Through this partnership, we have been able to reach students of diverse backgrounds and interests from across the great state of Virginia to not only bring awareness of cybersecurity and cyber careers, but also to build excitement about the future opportunities in the classroom.”*

G. B. Cazes  
Former Vice President  
Cyber Innovation Center

The camp design offered opportunities for guest speakers to share information about their cyber-related jobs, security in their companies, personal career paths, and what employers in this field look for in new employees. To understand the nature of cybersecurity work and the range of job opportunities that exist throughout the state, instructional teams planned cyber-

related field trips to government, financial institutions, companies, museums, and postsecondary institutions.

Counselors were involved in planning so that career activities would blend with the discussions in class, visits from speakers, and trips to cyber industries. LifeJourney, an online mentoring program, was offered as a resource for students to access video discussions of people in cyber careers. Instructional teams utilized the Virginia Career VIEW online program and used other career resources available in high schools. Counselors planned several career development activities each week of the camp.

It was important for students and teachers to learn about the types of industry certifications and educational levels that are required in cybersecurity careers. The camp design included time for students to work toward an industry certification that is recognized in the technology and cybersecurity fields. The Virginia Department of Education emphasized the importance of industry certifications by asking each camp to help students advance toward earning the IC3 Digital Literacy Certification. Teachers were not asked to “teach to” specific skills measured by this certification but rather to administer the certification exam as a pre-test in the first days of the camp. Results of a pre-test could help the instructional team understand the level of knowledge and skills the students had acquired prior to the beginning of the camp. The certification exam would be administered a second time at the end of the camp as a measure of the progress students were making toward completing the IC3 certification by the end of the 2016-2017 school year.

Each location planned to close the camp with a culminating program to give students a platform for demonstrating to parents and the community what they had learned about cybersecurity, coding, and careers. Students would receive a certificate of completion from the Virginia Department of Education and local programs could recognize students for other achievements during the CyberCamp Program.

# IMPLEMENTATION

## Campers learn to code, explore careers, and achieve an industry credential.

Virginia's CyberCamps were highly visible across the state throughout the summer as camps were conducted from mid-May through early August. The CyberCamp program was a pilot for the state, so it was important to learn whether the camps operated as planned, whether the NICERC curriculum was helpful, how students responded to the activities, and how teachers benefited from the camp experience.

The CyberCamps submitted their schedule of daily activities to the Office of CTAE. The learning activities were highly similar across camps. Instructional teams followed the guidance of the NICERC training staff and the Office of CTAE to include opportunities for learning that would build a foundation of knowledge and skills to understand cybersecurity and gain awareness of cyber-related careers.

CTE staff visited camps in several locations to learn more about the program. These staff had attended one of the NICERC professional development sessions in the spring, so they had a good understanding of the information teachers had received. Their observations confirmed that the camps were functioning well, students were participating in and enjoying classroom activities, and teachers were pleased with the progress being made.

To augment the planning documents and information from staff visits, an external researcher selected eight of the 32 CyberCamps (25 percent) to visit, one in each of the eight Superintendent's Regions. Camps were selected based on several criteria that would help provide a thorough description of the CyberCamp Program. The camps that were visited and the days they were visited were chosen because they represented

- Rural, suburban, and urban school divisions.
- Schools of different sizes.
- Camps for a single division and regional camps serving several divisions.
- Camps conducted in a high school and camps held in a career and technical center.
- Camps that were conducted at different times over the summer.
- Different daily and weekly schedules.
- Different points in time: the early days of the camp schedule, midway through the camp, and at the end of the camp.
- Ethnic/racial participation across the state.
- Different selection criteria for student participation.
- An opportunity to view all aspects of the camp program.

The researcher observed the entirety of the camp day, including classroom instruction, student project groups, and guest speakers; procedural activities, meals and breaks; daily closing activities; and student and teacher interaction. The researcher participated in field trips with two camps. She spoke with camp directors, individual teachers, teams of teachers, individual students, teams of students, and in some cases division leadership.

The report that follows combines the information gathered in written documents and visits by the researcher. The CyberCamps were highly consistent in the curriculum followed and instructional activities delivered. The learning environment was remarkably similar in each camp visited. This report presents descriptive information that is generalized for the collective pilot program. Observations of activities and comments from students and staff are used in conjunction with the planning documents to describe Virginia CyberCamp 2016 in action.

**Participation** – A total of 743 rising 10th-, 11th -, and 12th-graders participated in the CyberCamps. The enrollment goal for each camp was 25 students:

- 11 camps enrolled more than 25 students.
- Six camps enrolled 25 students.
- Five camps enrolled 21-24 students.
- Six camps enrolled 15-19 students.
- Four camps enrolled 12-14 students.

The composition of camps that were observed were almost 50 percent girls. Students reflected the ethnicities of their regions. Attendance was excellent for a summer program. There were instances of students leaving for a family vacation or missing a day for illness, but generally students were present throughout the camp and wanted to participate.

Most camps were conducted over four days for three weeks. Some camps ran over a longer number of days or chose to intensify the camp by operating five or six days a week. Typically, camps began early in the day with breakfast and continued until mid-afternoon. Schools either used the division's food service for meals or had meals brought in from area restaurants. Students commented that they appreciated the good quality of the food and the amount available. The school division hosting the camp provided bus transportation daily to the school and throughout the week for field trips.

**Teaching and Learning Environment** – The learning environment was noticeably different from a typical academic classroom. Rather than sitting in desks to work, students were free to move at will and work with other students as they desired – at tables, on the floor, alone, or in groups. The atmosphere was highly relaxed, yet the students were consistently working on assignments or projects. Students were outfitted in their CyberCamp shirts, each one unique to the camp.

The classes – be they in computer labs, classrooms, or large open spaces – reflected high student engagement in computer programming, projects, online learning, written and oral assignments, and guest speakers. Students were on task consistently in this relaxed but highly productive atmosphere. When asked what surprised them the most about the CyberCamp, students from each camp visited echoed the same response: *“I expected that we would sit in front of a computer while teachers lectured to us. It wasn’t like that. They let us be creative.”*

It was clear students enjoyed this way of interacting with new content. They were busy all of the time, working on team projects when they had extra time. Several students asked their camp director why they held the camp only four days a week instead of five, because they would have enjoyed more time to work together, and could they come back to the school after the camp to continue working.

Students preferred to solve problems by themselves or in small groups and asked teachers for assistance only after they had exhausted their resources. Students were observed in all camps using reference materials to search for programming information when they encountered a coding problem, rather than immediately asking a teacher for the right answer. When the robots didn’t perform as expected, students tried different procedures or sought help from a peer to get the desired result. One teacher commented that the students told her not to give them help because they preferred to find their own solutions when confronted with the unknown. Consistently, this was the students’ preferred way of working – independent of the teacher or collaborating with other students.

There were no disciplinary issues observed or shared by teachers. Students behaved in a responsible way while working on projects, taking breaks, and having meals. As a student commented, *“The camp provided a comfortable learning environment.”* One teacher was curious how a camper, who had slept through her class during the academic year, was so interested and performing so well in the camp.

Teachers presented new information or initiated an activity with the whole group, but quickly students were on their own or in teams to proceed on the tasks. Teachers were acting as facilitators of learning, not lecturing or imposing themselves on the students. They were present to answer questions and monitor the schedule for the day. Students appreciated seeing the teachers approach learning differently: *“I was surprised that the camp was so much fun – not so structured. The teachers were relaxed.”*

The teacher teams worked well together, sharing responsibilities and enjoying the cross-disciplinary approach to learning. As a teacher noted, *“I wish we could teach this way [cross-disciplinary] during the school year.”* When presenting new information, they shared the responsibility of leading discussions and explaining new tasks. The instructional team members were available as students worked, but often one teacher was clearly the lead, especially for the activities that involved writing or debate.

There was no noticeable difference in the comfort level of the CTE and academic teachers as they followed the NICERC curriculum and led projects. It appeared that the instructional team had benefitted from professional development and mastered the activities associated with the curriculum because academic as well as CTE teachers were observed helping with robots and troubleshooting coding errors.

Collectively, the planned camp activities can be grouped into three broad themes: Learning to Code, Exploring Careers, and Gaining Skills and Credentials.

**Learning to Code** – The CyberCamp scheduled the greatest amount of instructional time for activities related to understanding networks, building robots, programming the robots to accomplish tasks, and solving problems associated with robots and coding. Projects assigned to student teams utilized the robots and coding but also required students to use mathematics.

Camps spent the first week closely following NICERC’s recommended activities to review electricity, build robots, and immediately begin programming the robot and writing code. Concurrently, students began learning about opportunities, threats, responsibilities, and legal constraints associated with operating in cyberspace. By the second week, students were involved in projects that varied by camp, although they were highly similar in building capacity with coding and building an understanding of cybersecurity. Students were progressively giving more complex tasks to their robots to perform, and some students were programming the robots to go beyond their assignments. Heritage High School CyberCamp students programmed their robots to play music as the robots competed to negotiate an obstacle course.

Teachers were free to supplement the NICERC curriculum with cybersecurity activities from the CTE or academic program. Some programs integrated resources that accompany their engineering and technology programs using Raspberry Pi Computers and Hummingbird Robotics. A science teacher utilized her experience teaching biology to create a cybersecurity DNA activity.

The intensity with which the students attacked their coding assignments and group projects speaks to the commitment they showed to this learning opportunity. They appeared to take advantage of every opportunity given them to learn about networks and coding, and how what they were doing applied to hacking and security breaches. *“Learning to program the Boe-Bots was the best part of the camp!”*

Students were successful with the robotic activities regardless of prior learning or limited experience with computers. This is noteworthy as one camp chose engineering students for the camp, and their success with the instructional activities appeared no different than another camp that deliberately chose students that had no engineering instruction or camps that chose students regardless of their prior experiences.

**Exploring Careers** – Students had multiple opportunities to learn about careers in cybersecurity and other cyber-related jobs. First, counselors oversaw online learning that allowed students to explore job tasks, find education information, understand work values, and watch videos about jobs related to cybersecurity (e.g., programmers, software developers, computer network architects, security management specialists, special agents, and intelligence analysts).

Additionally, students interacted with individuals who came to the camps to speak about their jobs and the importance of security in their career fields. The speakers spoke candidly about the type of people they want to hire – both educational attainment and personal qualities, including the ability to receive a security clearance. These conversations were enhanced by field trips to businesses that require high levels of security or provide personal information security. For example, students toured corporate financial data systems, county technology centers, and energy companies that revealed the different ways data are secured, the threats of breaches and hacking and the resultant cost to the company and the society at large, and how specific jobs protect information. Camps visited colleges and universities to get a better understanding of cybersecurity courses and certifications as well as research being conducted.

Interactive activities and simulations enhanced field trips and visits to the classroom and provided a real-world cyber experience. A daylong visit to Radford University provided one camp with an opportunity to engage in a Capture the Flag cybersecurity competition. The professors stated that the high school campers performed as well as the college students. Several camps went to the International Spy Museum, where they were led through a realistic spy simulation activity. A representative from Naval Surface Warfare Center Dahlgren Division provided websites for students to access to practice cyber attacks. These interactive activities added value to the career-focused observations and conversations that occurred during the field trips, and the students enjoyed them: *“My favorite activities were the cyber-attack activities.”*

The following companies, organizations, and institutions provided tours, speakers, and activities during CyberCamp field trips. Some locations were visited by more than one camp.

Company, Organization, Institution	Location	Topic
<b>Banks and credit unions</b>	Various locations	Security in banking
<b>Battelle</b>	King George Arlington	Cybersecurity services
<b>Capital One</b>	Richmond	Data security
<b>Carowinds</b>	Charlotte, NC	Park security and networks
<b>Chatmoss Cable</b>	Martinsville	Tour
<b>Coesia</b>	Richmond	Tour

<b>Company, Organization, Institution</b>	<b>Location</b>	<b>Topic</b>
<b>Community colleges</b>	Danville John Tyler Lord Fairfax New River	Programming, cyber careers, security knowledge, online safety, college course offerings
<b>Convergent Technologies</b>	Winston Salem, NC	Cybersecurity awareness; Cyber threat security
<b>Naval Surface Warfare Center Dahlgren Division</b>	Dahlgren	Hacking
<b>FBI Field Building</b>	Manassas	Tour
<b>Fort Lee</b>	Petersburg	Computer war games and cybersecurity
<b>Google</b>	Washington, DC	Personal security
<b>HUMES Center</b>	Blacksburg	Ground Ops Station tour
<b>Institute for Advanced Learning and Research</b>	Danville	Data security
<b>International Spy Museum</b>	Washington, DC	Interactive spy experiences and team building
<b>Local police/sheriff departments</b>	Multiple	Cybersecurity awareness and data security
<b>County technology center</b>	Pulaski	Data storage and security
<b>Microsoft Data Center</b>	Boydton	Data processing security
<b>Museum of the U.S. Navy</b>	Washington, DC	Cyber technologies
<b>National Cybersecurity and Communications Integration Center (NCCIC), division of U.S. Dept. of Homeland Security</b>	Arlington	Malicious cyber activity awareness
<b>Neustar Inc.</b>	Sterling	Tour
<b>NIBCO</b>	Stuarts Draft	Robotic demonstration and programming
<b>Philpott Dam</b>	Bassett	Dam security
<b>Rolls Royce</b>	Prince George	Tour
<b>SD Solutions</b>	Luray	Federal elections security
<b>Symantec</b>	Herndon	Defense against viruses, spyware, malware, online threats
<b>Universities</b>	James Madison Norfolk State Radford Virginia Commonwealth Virginia State Virginia Tech	Capture the Flag competition, programming, cyber careers, security knowledge, online safety, university course offerings
<b>Virginia Bureau of Criminal Investigation</b>	Richmond	Bomb robot
<b>Virginia Science Museum</b>	Richmond	Robotics hands-on demonstration
<b>Virginia Tech Center for Dynamic Systems</b>	Blacksburg	Robotics lab tour
<b>National Weather Service Forecast Office</b>	Wakefield	Tour

One of the guest speakers was a member of Congress who spoke on cybersecurity awareness. Other guest speakers shared information about cyber-related careers, security in their company, what the security industry is doing, and what they look for in employees. The following companies and organizations were among those who supplied guest speakers:

- Capital One Data Center
- Comsonics
- Dominion Virginia Power
- ECPI
- Fairfield Echols
- Kirkland Mission Critical
- Union Bank
- Lockheed Martin
- Millennium Corp.
- Naval Criminal Investigative Service (NCIS)
- Northrop Grumman
- Pierce Matrix
- RPI Group Inc.
- U.S. Defense Commissary Agency
- U.S. Department of Defense
- U.S. Department of Homeland Security
- Valley Health
- Virginia Community College System
- Virginia Department of Juvenile Justice
- Virginia Information Technologies Agency
- Virginia State Police Cyber Crime

Collectively, the CyberCamps used the resources of educational institutions, security organizations, government agencies, banking, energy, and health to provide students with information about what is being done to address security needs, careers related to cybersecurity, and educational opportunities. The field trips were enjoyed by the students, as one camper commented: *“Loved the field trips. I expected to be told about cybersecurity, not free to work on it [during the field trips].”*

Conversations about careers in cybersecurity often dealt with the specific requirements for a type of job. Speakers never hesitated to discuss their career journey and the importance of being prepared to move into new jobs as their careers progressed. They shared how they worked with teams of workers, the hours they worked, and security clearance requirements to be considered for many jobs. Students received advice about how to proceed with decisions about their futures – getting involved with discussion groups in technology and obtaining the latest industry certifications. Speakers focused on the type of people that are successful in cyber-related jobs in their industry. Speakers emphasized that while students need education and skills, they must be prepared to be lifelong learners:

*“Technology is a treadmill. What you know today will be worthless in two years. Focus on learning. A new opportunity may seem like a burden but it prepares you for other things.”* – Financial Sector

*“It’s not what you know – it’s that you can learn.”* – Financial Data Sector

Students were told how important soft skills are, including writing, reading, and communicating, in any career:

*“I wouldn’t be in this job if I couldn’t communicate.”* – Aerospace Sector

*“We want workers who can multitask, communicate, and work in teams.”* – Safety and Security Sector

*“Be a reader. Read anything, because if you can read, you can write.”* – Military Sector

*“Learn to write convincingly.”* – Financial Sector

*“You need soft skills: self-direction, how to make yourself part of a team, and out-of-the-box thinking. You can’t shut down when things go wrong.”* – Aerospace Sector

*“You have to show that you have drive and desire.”* – Financial Data Sector

The continuous effort to expose students to cybersecurity careers paid off. Students engaged in online learning, were attentive to speakers, and took advantage of the field trips. They left the camp with more knowledge about careers, opportunities that are available in the state, and the steps they need to take to become qualified for a cyber job. When asked at the culminating event about her experience, a student said, *“What did I learn from the camp? I didn’t know there were so many careers related to cybersecurity.”* Teachers were engaged with speakers, as well, and it was apparent they were learning alongside the students. A camp director noted, *“The faculty and staff that participated in the CyberCamp stated that it was just as much a learning experience for them as it was for the students.”*

**Gaining Skills and Credentials** – During the CyberCamps, students heard from cybersecurity employers about the importance of education, including the necessity to earn industry certifications for many jobs in cybersecurity fields. The Virginia Department of Education designed the CyberCamps to include industry certification testing to demonstrate to students and teachers the value of associating one or more of these tests with any career pursuit. The Office of CTAE chose the IC3 Digital Literacy Certification<sup>1</sup> as the preferred certification examination to use with the CyberCamp program. The IC3 is used worldwide to validate digital skills of students and employees. IC3 is recognized by the International Standards for Technology in Education (ISTE), the American Council on Education (ACE), and the National Coalition of Certification Centers (NC3). IC3 is reviewed by the Global Digital Literacy Council.

---

<sup>1</sup> With more than three million exams delivered in 78 countries, the IC3 Digital Literacy certification has become a global standard for measuring and validating digital skills of students and employees all around the world. In addition, the American Council on Education recommends postsecondary credits in general education or computer literacy being awarded to students in possession of an IC3 certification.

Participants in Virginia’s CyberCamps had the opportunity to advance toward earning the IC3 Digital Literacy Certification, which requires passing exams in three key areas: Computing Fundamentals, Living Online, and Key Applications.

The **Key Applications examination** covers popular word processing, spreadsheet and presentation applications, and the common features of all applications.

The **Computing Fundamentals examination** covers a foundational understanding of computer hardware, software, operating systems, peripherals, and troubleshooting.

The **Living Online examination** covers skills for working in an Internet or networked environment and maximizing communication, education, collaboration, and social interaction in a safe and ethical way.

Each exam is independent (approximately 45-50 minutes each) covering separate objectives and validating specific areas of digital competency. A student may proceed to earn an IC3 certification by passing each of the three individual exams.

The Northern Neck Technical Center hosted two camps for six school divisions in the region. Of the 42 participants, 11 students passed the Living Online examination on the first testing. An additional 11 students passed this exam when they were tested near the end of the camp, so 52 percent of campers left the camp and began the school year with one of three areas of study of the IC3 certification completed. Overall, those students who were post tested demonstrated a 30 percent increase in their scores after less than 70 hours of instruction.

The CyberCamps offered students the opportunity to take the exams as pretests, to take individual exams at the end of the camp, and to earn an IC3 certification. Among 51 schools or education centers administering IC3 tests during the 2015-2016 school year and during the camps, 6,168 tests were administered, and 2,074 tests were passed. Of these 51 schools, 21 hosted camps and administered tests during the summer of 2016. These schools administered 1,397 tests between July 1, 2015, and July 30, 2016, of which at least<sup>2</sup> 980 were administered as a result of the camps, which is 15 percent of the test taking done throughout the entire year. It is notable that as the result of a 70-hour program, the CyberCamps contributed at least 253 additional tests passed – 12 percent of tests passed through the regular school term.

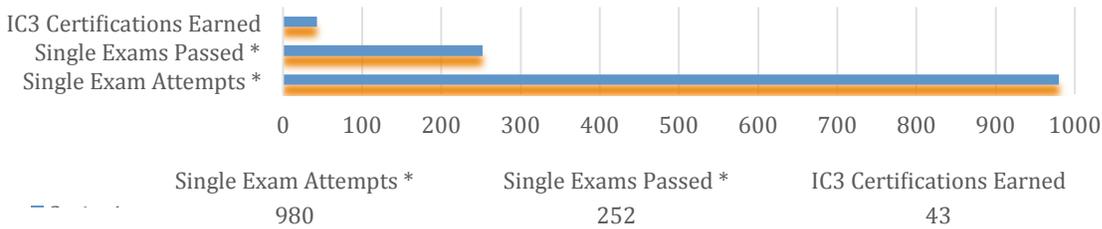
By the completion of the camps, students had taken 980 single exams and had passed 252 single exams. Forty-three students passed the three areas of study (three single exams) and earned the IC3 Digital Literacy Certification by the camp’s completion.

---

<sup>2</sup>The figures cited “at least” exclude tests administered and tests passed at those schools with *both* testing during the school year and a camp. We are unable to isolate the contribution made by the camps to those schools with existing IC3 testing regimens.

The following are the testing results for all camps combined:

### CyberCamp 2016 Credentials Results



The performance of campers on the IC3 exams offers potential for growth. Given the short time frame of the camps, only exceptional students, or those who had already completed some of the exams in the school year, would be likely to complete all three exams.

There is significant growth potential, however. The introduction to Computing Fundamentals is a gateway for students to understand the digital world in ways essential to workforce or higher education readiness. Each student has the opportunity to continue working toward the IC3 certification encompassing all three areas of study should they have only passed one or two of the three exams required during their CyberCamp.

# IMPLICATIONS FOR FUTURE PROGRAMS

## Positive results give direction for future cyber programs.

The description of the 2016 CyberCamps Program and the supportive data from the industry certification testing paints a positive picture of students statewide learning new information and gaining skills. Further analysis of the camp observations helps to refine this picture, so that the Virginia Department of Education can begin to determine first, whether the program met its goals and, second, if the program is determined to have been beneficial to students and teachers for more than the short term. In drawing these conclusions, it is useful to make recommendations applicable to future cybersecurity education initiatives, especially as the cybersecurity career pathway is incorporated into CTE program areas.

**What Was Learned – CTE staff provided a strong and workable framework for developing the camps.** Cybersecurity education is new to most schools in Virginia. Perhaps the greatest challenge presented by this initiative was asking teachers from divisions across the state with no background in cybersecurity, computer programming, and cyber career awareness to develop the camp program. The CTE staff was deliberate in making decisions about the Virginia CyberCamp 2016 Program and based them on the following assumptions:

1. It is important to have consistency in the instructional programs delivered in every site. The curriculum for the camps should be highly similar so that comparisons in outcomes can be made.
2. Any program that has the potential to influence new courses and greater opportunities for earning industry certifications must be of high quality and should be research-based.
3. The Office of CTAE should identify curriculum resources and make available professional development to provide the members of the instructional team of each camp with the tools they need to teach cybersecurity with confidence.
4. The budget should be adequate to cover all costs.
5. Each CyberCamp should include the expertise of local colleges and universities, as well as nearby companies and institutions that have cybersecurity-related careers.

The 32 camps followed state guidelines to create cybersecurity programs and to operate the camps as an extension of the 2015-2016 school year. This was no small accomplishment, because in less than six months each division hosting a camp completed the following:

- Completed intent and application forms.
- Received notification of selection as a CyberCamp.
- Selected camp staff from academic, CTE, and counseling staff who would agree to plan and work in the camp (without first reviewing a curriculum).
- Participated in professional development to learn to teach the NICERC Cyber Literacy curriculum, which included computer programming and robotics, liberal arts lessons related to cybersecurity, and cyber ethics.
- Planned the instructional program the camp would deliver, including assigning lead teachers for topics, becoming comfortable with robotics, and developing an understanding of cross-disciplinary teaching and learning.
- Developed the guidelines for the camp and requirements for student participation.
- Informed the School Board and community about the program.
- Recruited students.
- Purchased materials and planned all logistics, such as transportation and meals.
- Understood how to administer the IC3 certification exams.
- Coordinated with other divisions if they were developing a regional camp.
- Secured computers and adequate space for camp activities.
- Identified field trip opportunities and guest speakers within driving distance and selected dates for their participation.
- Chose the date and schedule for the camp, taking into consideration other activities at the school, such as summer school programs.
- Prepared a schedule of all activities by day and submitted it to the Office of CTAE for review.
- Finalized the budget.

Each camp provided the required 70 hours of instruction, and some camps exceeded it. There appeared to be no logistical issues as the camps followed their schedules and completed their camps with good participation from students.

**What Was Learned – The instructional teams benefited from the professional development that was provided by NICERC staff.** The Office of CTAE was successful in providing a strong cyber literacy curriculum and excellent professional development, as was evident in the competent way the school teams delivered the instructional activities. The teachers did not appear to be novices teaching programming or working with the robots. The instructional teams displayed great enthusiasm for the content, and taught the curriculum as the NICERC

staff had modeled. Teachers thought the professional development they received was very good. The decision to partner with NICERC was an excellent decision, as the NICERC staff proved to be highly competent, well-prepared trainers who were available throughout the summer for any needed support. For example, at one camp, the students were able to complete planned activities faster than anticipated by the teachers, so a teacher contacted NICERC and received additional activities to incorporate immediately.

**What Was Learned – The cross-curriculum teaching staff contributed positively to the instructional program.** Teaching as a team was new to the instructional teams, and academic teachers working with CTE teachers in a CTE program was foreign to everyone. Using the integrated units of instruction that NICERC provided, teachers planned together and “figured out” how to approach teaching in a collaborative team environment. Many teams talked about how they liked working this way. It was clear that the academic teachers learned a lot about cybersecurity and were thinking about how to integrate it into the regular academic curriculum. It was impressive that English teachers were able to see the value of adding topics related to the world of work, especially in their choice of books to read and writing assignments to give.

The weakest link in the instructional teams appeared to be school counselors. At some camps, they were only present when they made a presentation using Virginia Career VIEW or were participating in a field trip. Other counselors were present but did not seem to have a strong role. Even though a counselor’s role is to provide guidance and advisement related to career planning, the assumption cannot be made that they are aware of cybersecurity or IT careers that exist or are aware of opportunities for employment throughout Virginia.

**What Was Learned – The orientation to careers in cybersecurity varied greatly across the state due to the dependence on outside speakers and field trips for information.** Whereas the NICERC curriculum prepared teachers for important topics in cyber literacy to include in the camps, the counselors did not receive specific training or resources related to cyber careers. They had an opportunity to use Life Journey online, but no one was observed using it. Therefore, information about working in cybersecurity was dependent on speakers. As explained in this report, the students received good information from some speakers, but each camp interacted with different people, and no attempt was made to capture everything that occurred on each field trip or during a guest presentation.

**What Was Learned – Teachers’ awareness of cybersecurity-related jobs in Virginia and the education and training required for employment in these fields increased because of the camps.** There is little doubt that each teacher and school leader involved with the camps

*“The camp has helped us see that we need to offer more courses in both cybersecurity and computer science. The core group of my campers have been very willing to meet during the school year as almost an unofficial club. The faculty members have a much better understanding of why we need to have additional cyber courses and how they can include cybersecurity in their curriculum to not only help keep kids safe, but to spark their interest as well.”*

CyberCamp Director,  
County School Division

learned as much about careers and the education required for specific jobs as the students. Teachers were as attentive on field trips and with speakers as the students were.

**What Was Learned – Employers and higher education faculty played a supportive role in the camps.** There was no evidence that instructional teams used employers or faculty members to help plan the camps. Both groups were used to provide field trips and speakers, and their role should not be minimized. However, school teams appeared not to include anyone outside of the school in developing the camp.

**What Was Learned – Choosing field trip locations and guest speakers was done without as much information as the instructional teams would have liked.** While most field trips and speakers were contributors to the program, teachers said if they were to plan another camp they would want to start planning early in the year so they could be more strategic in their selections. They wanted to know the companies or locations that other camps visited, hoping to build a resource list of places and people in Virginia that work with cybersecurity.

**What Was Learned – Some camps had to work hard to recruit participants for this new program.** Other camps reached their target or had to select from more applicants than they could serve. All of the sites visited indicated that they would like to continue offering a CyberCamp and thought they would have no trouble recruiting a second year. Students said they would promote the camp with their peers.

**What Was Learned – The high engagement of students in all camp activities is noteworthy.** At a time when many schools struggle to engage students in learning, the CyberCamps captured the students' interest and held it throughout the length of the camps. Clearly the students were interested in the coding activities and group projects – that was observed in each camp. But the students pointed out that they felt they could be creative in this environment, which surprised them. Their creativity was encouraged as they engineered new tasks for their robots and they looked for interesting ways to work on projects.

Students also were highly engaged when speakers talked about careers; also when they visited high-profile companies such as Microsoft, had the state's bomb robot visit them, listened to a representative from NCIS talk about forensics, and heard Google staff explain why students should change their passwords. The relevance of the camp curriculum, the freedom given to students to move around the class space, encouragement to be creative, and the independence given to individual students and teams appeared to contribute to the high interest students showed in the program.

**What Was Learned – Watching students work collaboratively on projects in the camp environment replicated millennial IT workplaces.** Companies such as Google and Rack Space in Blacksburg have created workspaces that support their philosophy that happy workers are

productive workers, so they provide the personal supports that they appreciate. Viewing students in the camps as they moved around at will, stopping for breaks and immediately returning to work, and expressing their appreciation for good food – and a lot of it – is highly similar to the work environment in some of the new IT workplaces. This unanticipated, incidental learning may help inform teachers who are interested in creating more engaging learning environments. Also, this information can be shared with students to describe the new millennial workplaces in which many of the IT and cyber-related jobs are located.

**What Was Learned – The extended school year opportunity and intensive time to work on cyber literacy may have influenced the high level of interest shown by students.** As students worked on group projects for a couple of hours without interruption, it was noted that this would not have happened in an academic class due to the typical 55- to 85-minute class period. CTE classes are usually blocked for longer instructional periods. Projects take time, and students need time to work through problems without stopping to move to a new activity. While some of the more complex robotic builds may take longer than one traditional or block class period, the pacing is such that these projects are given multiple class periods to complete. This adjustment proves useful when including these projects in a class schedule or the summer camp experience.

**What Was Learned – Academic teachers reported that they will incorporate some of what they experienced in the camp in the regular academic program.** When asked about the influence of the camp experience on their planning for the next academic year, some teachers expressed an interest in incorporating cybersecurity into their academic courses. As no attempt was made to follow up with teachers, there is no way to know the extent cybersecurity is being integrated into the regular English, science, or mathematics SOL curriculum.

**What Was Learned – The cybersecurity curriculum taught in the camp program and the materials purchased for the camp are likely in use to some extent in each high school during the 2016-2017 year.**

Camp directors were excited about having the resources of the camp available for other CTE programs, such as robotics and IT courses. Additional resources purchased for the camps, such as Hummingbird robotics, strengthen the CTE course offerings and encourage teachers to weave in information about cybersecurity as they teach various units of study. The NICERC curriculum serves as an excellent resource for designing new cybersecurity courses, which are likely to increase when CTE announces the cybersecurity career pathway.

*“This camp experience truly opened our students’ and faculty’s eyes to the amazing and plentiful career opportunities that are available in cybersecurity. We are planning to have another camp, have begun establishing a cybersecurity class that will be offered next year, and are using the NICERC curriculum as a supplement in our programming and coding class.”*

CyberCamp Director,  
City School Division

### **What Was Learned – The goals of the Virginia 2016 CyberCamp Program were met.**

- There was an increase in awareness of careers in cybersecurity among teachers and students. This occurred because camp activities revolved around an understanding of cyber careers: (1) discussions in class while coding, working on projects, writing papers about security issues, and debating ethical issues; (2) field trips to cyber-related companies and companies that are faced with security challenges; (3) speakers that shared their career experiences and education; (4) visits to colleges and universities; and (5) use of online career information systems.
- Students were engaged in project-driven learning using the NICERC curriculum in a positive, student-friendly environment.
- Students and teachers were introduced to cybersecurity-related industry credentials through the administration of the IC3 Digital Literacy examination. Teachers learned what content is measured on that certification exam. Forty-three camp participants earned the IC3 Digital Literacy Certification and 252 passed a single exam. Each student had the opportunity to continue working toward earning the IC3 Certification during the 2016-2017 school year.

## RECOMMENDATIONS FOR NEXT STEPS

To build upon the success of the camps and use the findings to support the implementation of the cybersecurity career pathway, the following actions are recommended for consideration:

1. Publish a brochure that highlights the components of the CyberCamps to assist schools that are interested in developing a camp or after-school program.
2. Continue to partner with NICERC to offer professional development on the cyber literacy curriculum in Virginia locations.
3. Provide professional development for school counselors on cybersecurity to strengthen their knowledge base as the cybersecurity career pathway is implemented.
4. Create support for cybersecurity competitions that are held throughout the state.
5. Provide information to school counselors and instructional staff on cybersecurity resources, industry certifications, courses, and majors that are available through community colleges and universities.
6. Create a short paper or brochure on cross-disciplinary teaching, asking a few of the CyberCamp academic and CTE teachers to share their perspective on the value of this methodology.

7. During the roll-out of the cybersecurity career pathway, provide information to academic teachers, including teachers of computer science.
8. Create a list of the companies, educational institutions, agencies, and other organizations that participated in the CyberCamps and distribute it to schools interested in developing a camp and as a resource to CTE programs that need to expand their advisory boards to include representatives from cybersecurity fields.

## Works Cited

- Armstrong, D. K. (2015, August 27). *Cybersecurity Regulation of Wireless Devices for Performance and Assurance in the Age of "Medjacking."* Retrieved August 22, 2016, from Journal of Diabetes Science and Technology:  
<http://dst.sagepub.com/content/10/2/435.abstract>
- Buchanan, L. (2017, January 18). *Cybersecurity Games: Building Tomorrow's Workforce.*
- Bureau of Labor Statistics, U.S. Department of Labor. (2015, December 17). *Occupational Outlook Handbook 2016-2017 Edition.* Retrieved November 13, 2016, from Information Security Analysts: <http://www.bls.gov/ooh/>
- Cisco. (2015). *Mitigating the Cybersecurity Skills Shortage: Top Insights and Actions from Cisco Security Advisory Services.* Retrieved November 13, 2016, from Cisco:  
<http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf>
- Fanelli, B. P. (2016, Fall). *The State of Cybersecurity Among Small Businesses in North America.* Retrieved November 13, 2016, from Council of Better Business Bureaus Inc.:  
<http://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/cybersecurity-research-report.pdf>
- Goodman, M. (2015, 2016). *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World.* New York: Anchor Books.
- Institute, P. (2016, February). *The State of Cybersecurity in Healthcare Organizations in 2016.* Retrieved November 13, 2016, from ESET:  
[https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State\\_of\\_Healthcare\\_Cybersecurity\\_Study.pdf](https://cdn2.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf)
- Katzcy Consulting. (2016, November 1). *Cybersecurity Games: Building Tomorrow's Workforce.* Retrieved December 2016, from Katzcy Consulting:  
<http://lp.katzcy.com/cybersecuritygames>
- LeClair, J. A. (2016). *Women in Cybersecurity.* Albany: Hudson Whitman/Excelsior College Press.
- Lindberg, M. (2015, February 12). *3 Reasons We Want to Introduce Girls to Cybersecurity.* Retrieved November 13, 2016, from AAUW Careers and Workplace:  
<http://www.aauw.org/2015/02/12/introduce-girls-to-cybersecurity/>
- Margolis, J. (2008). *Stuck in the Shallow End: Education, Race, and Computing.* Retrieved November 13, 2016, from ACM Digital Library:  
<http://dl.acm.org/citation.cfm?id=1413116>

- Market Research Media. (2016, September 5). *U.S. Federal Cybersecurity Market Forecast*. Retrieved November 13, 2016, from Market Research Merdia: <https://www.marketresearchmedia.com/?p=206>
- Morgan, S. (2016). *Cybersecurity Jobs Report*. Retrieved November 13, 2016, from Cybersecurity Ventures: <http://www.cybersecurityventures.com/jobs>
- Morgan, S. (2016, January 2). *One Million Cybersecurity Job Openings in 2016*. Retrieved November 13, 2016, from Forbes: <http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#73b52e577d27>
- National Initiative for Cybersecurity Careers and Studies. (2016, November 3). *Department of Homeland Security*. Retrieved November 13, 2016, from Cybersecurity Workforce Framework: <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>
- Paul, A. (2016, August). The Coding Revolution. *Scientific American*, 315(2).
- Raytheon and National Cybersecurity Alliance. (2016, October). Retrieved November 13, 2016, from Securing Our Future: Closing the Cybersecurity Talent Gap: [http://www.raytheoncyber.com/rtnwcm/groups/corporate/documents/content/rtn\\_335212.pdf](http://www.raytheoncyber.com/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf)
- Schlesinger, J. (2015, August 26). *The Growing Need for More Women Cybersleuths*. Retrieved November 13, 2016, from CNBC Technology: <http://www.cnbc.com/2015/08/26/the-growing-need-for-more-women-cybersleuths.html>
- Smith, M. (2016, February 30). *Computer Science For All*. Retrieved November 13, 2016, from the White House: <https://www.whitehouse.gov/blog/2016/01/30/computer-science-all>
- U.S. Bureau of Labor Statistics. (2015, December). *Occupational Employment Projections to 2024*. Retrieved Released December 8, 2015, from Monthly Labor Review: (U.S. Bureau of Labor Statistics, 2015)
- Virginia Economic Development Partnership. (2016). *Virginia's Cybersecurity Industry*. Retrieved January 21, 2017, from YesVirginia.Org: <http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf>

# Notes for Planning Your CyberCamp:







© 2017 Commonwealth of Virginia Department of Education

*The Virginia Department of Education does not discriminate on the basis of race, sex, color, national origin, religion, sexual orientation, gender identity, age, political affiliation, or against otherwise qualified persons with disabilities. The policy permits appropriate employment preferences for veterans and specifically prohibits discrimination against veterans.*