Virginia's 21st Century Career Pathway

CYBERSECURITY

Virginia Department of Education
Richmond, Virginia

Virginia's 21st Century Career Pathway: Cybersecurity

Developed by the
Office of Career and Technical Education
Virginia Department of Education
Richmond, Virginia

© Virginia Department of Education, 2016

Copyright © 2016
Virginia Department of Education
P.O. Box 2120
Richmond, VA 23218-2120

Notice to the Reader

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.

Contents

Acknowledgements ..... **vii**

Introduction **1**

Meeting the Growing Demand **3**
Trends Related to Cybersecurity 4

Examining Needs of the Work Force **6**

Supplying Education and Training **11**
The Federal Call for More Education 11
How to Build Qualifications for Cybersecurity Careers 13

Developing a Course Framework **23**
Standards and Competencies 23
Organizing Principles 24

Taking Immediate Action **27**
Increase Knowledge 27
Review Current Practices 27
Secure Talent 28
Identify Resources 29

Works Cited **30**

Tables and Figures

Figure 1: Current and Projected Employment in Cybersecurity in Virginia 7

Figure 2: Percentage of Employment-based (H-1B) Visas Issued in Virginia by Occupation 8

Figure 3: Earnings and Growth for Selected Occupations in Virginia 9

Figure 4: Predominant Educational Level for Cybersecurity 12

Table 1: Enhancing Opportunities for Cybersecurity Careers at Virginia Colleges and Universities 14

Acknowledgements

Appreciation is expressed to the following individuals who contributed to the development of this document.

Principal Investigator
Dr. Yvonne V. Thayer, VESTED Educational Development

Demographic Research Group, Weldon Cooper Center, University of Virginia
Annie Rorem, Policy Associate
Dr. Meredith Gunter, Outreach Director

CTE Resource Center
Kevin Reilly, Administrative Coordinator
Jennie W. Blizzard, Writer/Editor

Virginia Department of Education
Dr. Steven R. Staples, Superintendent of Public Instruction
Dr. John W. Haun, Chief Academic Officer/Assistant Superintendent for Instruction
Bobby Keener, Chief Technology Innovations Officer
Brian Gibbs-Wilson, Chief Data Security Officer

Office of Career and Technical Education
Lolita B. Hall, Director
George R. Willcox, Coordinator for Planning, Administration and Accountability
Sharon W. Acuff, Marketing and Related Clusters Specialist
Dr. Lynn Basham, Technology Education and Related Clusters Specialist
Helen G. Fuqua, Family and Consumer Sciences and Related Clusters Specialist
Michele Green-Wright, Health and Medical Sciences and Related Clusters Specialist
Judith Sams, Business and Information Technology and Related Clusters Specialist
J. Anthony Williams, Trade and Industrial Education and Related Clusters Specialist
Carly Woolfolk, Agricultural Education and Related Clusters Specialist

A special thanks goes to the following cybersecurity experts for providing their expertise and input in the development of a cybersecurity curriculum:

G.B. Cazes, Vice President, Cyber Innovation Center
Kevin Nolten, Director of Academic Outreach, Cyber Innovation Center
Michael Miklich, CEO/President, Cybersecurity Education, Incorporated
Ray Kinard, Director, Cyber Academy, Northrop Grumman
Gen. Bernard Skoch, National Commissioner, CyberPatriot-Air Force Association
Drexel N. Harris, Recruiting/Sourcing Program Director, Dominion Resources
Ron Martin, Network/Telecom/Security Manager, Virginia Credit Union
Linda Lau, Ph.D., Associate Professor of Information Systems and Security, Longwood University
George Hsieh, Ph.D., Professor, Department of Computer Science, Norfolk State University
Edna Reid, DLS, Associate Professor, James Madison University
Cyndi Miracle, Senior Vice President-Research and Special Initiatives, Virginia Chamber of Commerce
Linda Lavendar, Business and Information Technology Teacher, Virginia Beach Public Schools
Megan Healy, Assistant Vice Chancellor for Academics, Virginia Community College System
Elizabeth Scruggs, Associate Director, Cyber Engineering Department, The Aerospace Corporation
Ross D. Matney, Career and Technical Education Director, Pulaski County Public Schools
Katie Rice, CTE/STEM Supervisor, Shenandoah County Public Schools

This document has been edited and produced by the
Office of Career and Technical Education
Virginia Department of Education
P.O. Box 2120
Richmond, Virginia 23218-2128
Lolita B. Hall, Director

CTE Resource Center
2002 Bremo Road, Lower Level
Henrico, Virginia 23226
Kevin P. Reilly, Administrative Coordinator
Jennie Blizzard, Writer/Editor

Introduction

In February 2014, Governor Terry McAuliffe established Cyber Virginia and the Virginia Cyber Security Commission through Executive Order 8. Among the responsibilities of the commission is to present recommendations that foster an improved cybersecurity workforce pipeline. This pipeline begins with K-12 education and continues through the commonwealth's many postsecondary education opportunities.

> *"Focusing on cutting edge education and training will be essential for Virginia's cyber security workforce and economic development as occupations in the cyber security industry are highly in demand and among the fastest growing in the economy."*
>
> **Virginia Gov. Terry McAuliffe Executive Order No. 8 (2014)**

There is an immediate need to identify the role of K-12 education in building the cybersecurity pipeline and to help schools at all levels – elementary, middle, and high school – prepare students for this new and important career field. In support of Governor McAuliffe's emphasis on cybersecurity in the commonwealth, this white paper highlights current efforts in cybersecurity education and serves as a call to action for Virginia's K-12 community of employers, educators, and citizens who are committed to the development of career and technical education programs.

PRIORITIES

Virginia currently faces an immediate and exciting opportunity to create a pathway to cybersecurity careers in Virginia, throughout the nation, and across the world. Community colleges and universities have begun to meet this challenge. What is lacking is a K-12 starting point for a career pathway to meet Virginia's cybersecurity workforce demand. This demand requires attention to the following priorities:

1 Identify stakeholders to develop a plan for cybersecurity education.

Individuals with expertise and experience from private industries and government agencies working in cybersecurity at various levels will be identified to articulate workforce needs.

2 Create a collaborative with Virginia's community colleges and universities.

It is imperative that any efforts to initiate a career pathway in K-12 dovetail with what postsecondary institutions offer and plan to offer in the future. Representatives from school divisions, community colleges, four-year colleges and universities, and the Virginia Department of Education should work together to set appropriate goals for K-12 cybersecurity education.

3 Develop one or more career pathways for cybersecurity careers.

The development of a cybersecurity pathway will require the insights of experts in related career sectors to confirm core cybersecurity competencies.

4 Secure instructional resources for a world-class cybersecurity initiative.

Cybersecurity programs require instructional resources because of the technical nature of the field. Curriculum frameworks will be developed and correlated to instructional resources and professional learning experiences. Students have the opportunity to earn industry-recognized credentials.

Meeting the Growing Demand

Since the beginning of the 21st century, the nation has experienced the impact of a technological revolution. Some refer to technological advancement as a "disruption" to the way we went about working and conducting business. In fact, technology has "disrupted" every career in some way – be it in the advanced speed of access to information, the analysis of critical data, or the development of tools that alter the way work is conducted. Technological advancements have created different expectations for many jobs, while increasing work output by offering quick access to information, tools to improve work processes, and opportunities to telecommunicate. With communication expedited through smart mobile devices and social networking, customers' expectations have changed as well as access to information about almost anything. Communication with most anyone is only a click away.

"A career pathway in cybersecurity is vital to establishing the robust talent pipeline needed to meet the growing demand for highly-skilled cybersecurity professionals. In addition to developing an understanding of the fundamentals of cybersecurity and information assurance, the curriculum should also seek to develop and enable practical application of related skills such as critical thinking, teamwork, conducting research, and self-motivation."

Marc Gaudette
Director,
IT Risk Management,
Dominion Resources

The role technology has played in the 21st century workplace cannot be overstated because of its influence on the workplace and the way the workforce is trained. Over the last three decades, technology has influenced how we prepare students for careers that comprise Virginia's nationally recognized 16 Career Clusters. Funds have been dedicated to provide the infrastructure, hardware, and software needed for workforce readiness across career clusters. Simultaneously, courses have been created in high schools and postsecondary institutions to develop the technical skills that are needed to understand technology and prepare for its application in the workplace. When we educate K-12 students for careers, technological applications are a component of the instructional design of any career pathway, including robotics in agriculture, big data networks in finance, video engineering in the arts, and diagnostic tools in health.

Another consequence of the technological revolution that has influenced the world of work is the creation of entirely new careers related to the field of technology. Careers in cybersecurity, in particular, have received national attention. These jobs continue to depend on computer science, engineering, and information technology education but also require workers who possess a highly creative set of skills to forecast the future of technology. Those with careers in cybersecurity work to predict and stay ahead of probable criminal activity as well as respond to it quickly when it happens.

Government, defense contractors, and privately resourced companies—all of which have

demonstrated a need for well-trained cybersecurity professionals—are densely clustered in Northern Virginia, Maryland, and Washington, D.C. As a result, Virginia has both an opportunity and a responsibility to prepare its young workers for these careers. Such preparation should include educating students on training requirements and required skills, providing them with options to participate in corporate-sponsored internships, and encouragement to begin working in government or private settings immediately upon completing educational requirements.

There appears to be no end to the growth of the cybersecurity industry. The 2014 tally of 300 cybersecurity companies in Virginia is growing to include a variety of companies looking beyond federal contracts for sustainability. In the last two years alone, the Northern Virginia Accelerator Program has ushered in 22 startup companies, which use private investment to increase sustainable businesses. The startups contribute to the field of larger security companies in their efforts to build privacy tools, create software to identify vulnerable parts of networks, plan recovery from attacks, oversee technology for cars, and test mobile applications. Even insurance companies may join the cybersecurity network as Virginia's smaller companies seek cyber insurance policies that can protect them from a devastating single attack (Cragle, 2015). Continued growth in companies that provide cybersecurity services means greater numbers of jobs will be created, adding to the existing number of jobs that are challenging an undereducated and undertrained workforce.

TRENDS RELATED TO CYBERSECURITY

The hacking of networks in business and government can lead to a range of information security threats, including criminal activity, espionage, terrorism, and warfare. Among the cyberattacks in the last year were (1) a data breach on Anthem Inc. health insurance that exposed the personal information of 80 million subscribers; (2) an attack on Home Depot that revealed 56 million customers' credit card information; (3) a malware infection that yielded customer information from 395 Dairy Queen restaurants; and (4) an Internal Revenue Service attack that resulted in $50 million in fraudulent tax returns (New York Times, 2015) (Mashable, 2015) (Riley, 2014). However, cyberattacks are not limited to large corporations, government, or chain stores. In 2014, 60 percent of targeted attacks struck small- and medium-sized organizations. Attacks are increasing, and in some cases stolen files have been held for ransom (Symantec, April 2015).

As security and technology experts from government and corporations shared at the 2015 National STEM Forum on Security Risks and Emerging Workforce Solutions, "It's not if you're going to be attacked – it's when you're going to be attacked."

As a consequence of these events and others, the ongoing connection between technological innovation and security threats to individuals and the nation is now widely acknowledged. And, as for individual security, no longer are laptop computers or smartphones the only source of potential security breaches. The evolution of smart devices, such as smart televisions, wearable activity trackers and watches, digital home thermostats and smart appliances, and navigation and entertainment systems in cars, has created a new opportunity to identify and share personal information.

Unlike the office computer, smart devices such as home security systems are a part of our lifestyle and are not shut down at the end of the day. Many smart devices function around the clock, maintaining connectivity to personal information that can be intercepted and used in unintended ways. In fact, networking technologists forecast that by 2020, 50 billion devices will be connected to the Internet (Elazari, 2015). These products and others with embedded computers and Internet connectivity offer advanced features, while presenting a heightened security challenge. It is in the best interest of our country to recognize the urgency of developing and supplying security services as quickly as new technological applications are created, thereby continuing to create jobs that demand cybersecurity skills.

In 2013, the IBM Center for Applied Insights conducted a study to understand how cybersecurity academic programs are evolving to meet increasing security threats. Faculty members from six countries identified four trends in cybersecurity education (Viveras, 2013):

1. **Information security is increasing in relevance.** Information security affects people every day and has become personal.

2. **There is increasing attention and demand from students, private industry, and government agencies.** Training an expert cybersecurity workforce is now a national priority. Rising demand is prompting the creation of more programs at universities, community colleges, and specialized technical schools.

3. **The field of cybersecurity has also significantly expanded with more domains to secure and more ways to attack.** There is more to teach and learn, and university programs are expanding.

4. **Academic programs are moving away from teaching purely the principles and theory of security to focus more on the practices.** This is largely driven by the demands of industry and governments, as well as by students who want to focus on real-world problems.

The big ideas in these trends call for immediate attention to developing a cybersecurity career pathway that can lead the way to more prepared workers for the growing career opportunities both in Virginia and across the nation. This paper discusses skills required for a workforce well-trained in cybersecurity; the education and training that will promote these skills, including a description of existing programs; and considerations for developing a cybersecurity preparation program within the context of career and technical education, including a list of targeted recommendations.

Examining Needs of the Work Force

As greater attention is paid to cybersecurity and the prevention of attacks, cybersecurity has become an industry with many types of jobs, creating the need for a growing cybersecurity workforce. The Council on CyberSecurity, a Washington-based nonprofit organization committed to the security of the Internet and elevating the competencies of the cybersecurity workforce, states that there is "an unprecedented demand for highly-skilled practitioners capable of building security into new and existing networks, assessing security on a real-time basis as new vulnerabilities are identified and disclosed, and acting as front-line cyber defenders across various industries and government agencies" (Council on CyberSecurity, 2015). Raytheon, with 21 Virginia locations specializing in defense, civil government, and cybersecurity markets, reports that there is an explosion in the cybersecurity area due to an increase in attacks and the sophistication of the attackers (Revere Digital LLC, 2015).

> *"All organizations have something to protect. As such, cybersecurity has become a required skillset in all functional areas of today's organizations. Therefore, the demand for knowledge and experience in this area will certainly grow and will require continuous learning."*
>
> **Jane Watkins**
> **President and CEO,**
> **Virginia Credit Union**

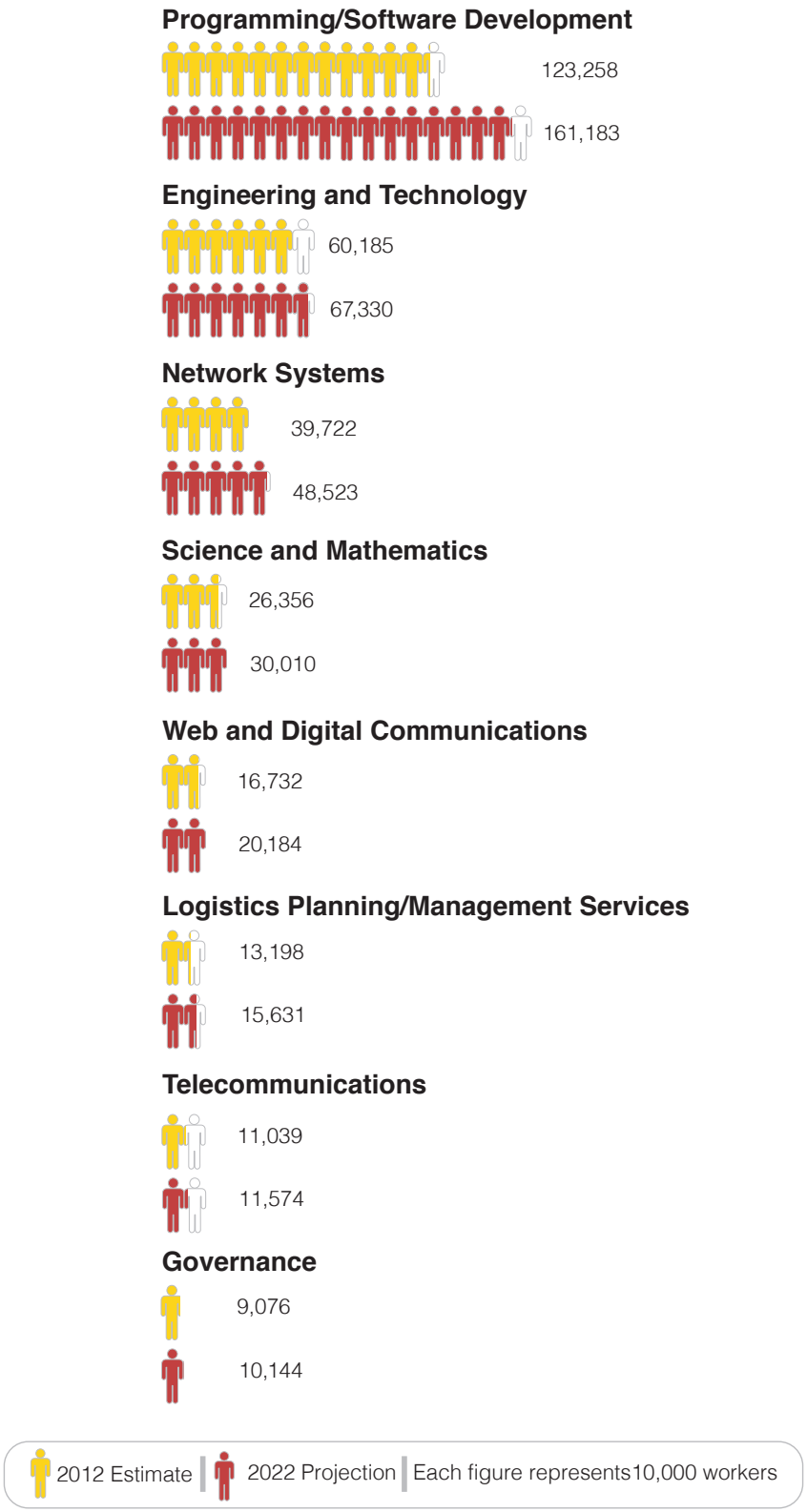
The number of cybersecurity jobs grows each year, but many of them remain unfilled due to an insufficient pool of candidates. Experts say there are more than 200,000 jobs in the U.S. unfilled, with an anticipated shortfall of 1.5 million jobs globally within five years (Frost & Sullivan, 2015). The Department of Homeland Security predicts that workforce developers should prepare for 2.5 million new cybersecurity positions (Scribner, 2015).

Cybersecurity jobs are expected to continue growing both to address the expansion of online businesses and to help federal agencies thwart cyberattacks, which exceeded 106,000 last year (Marsan). At the National STEM Forum on Security Risks and Emerging Workforce Solutions, it was predicted that within five years every business regardless of size would have to address their own internal security risks (STEMconnector, 2015).

What is the strength of Virginia's cybersecurity workforce compared to other states? The Cyberstates report (CompTIA Properties LLC, 2015) annually provides employment data comparing states engaged in technology industries. The latest report indicates that Virginia has 19,314 technology companies and 280,906 technology occupations. Data in the 2015 report reveal that Virginia has a concentration of 9.4 percent high-technology workers compared with 5.7 percent nationally.

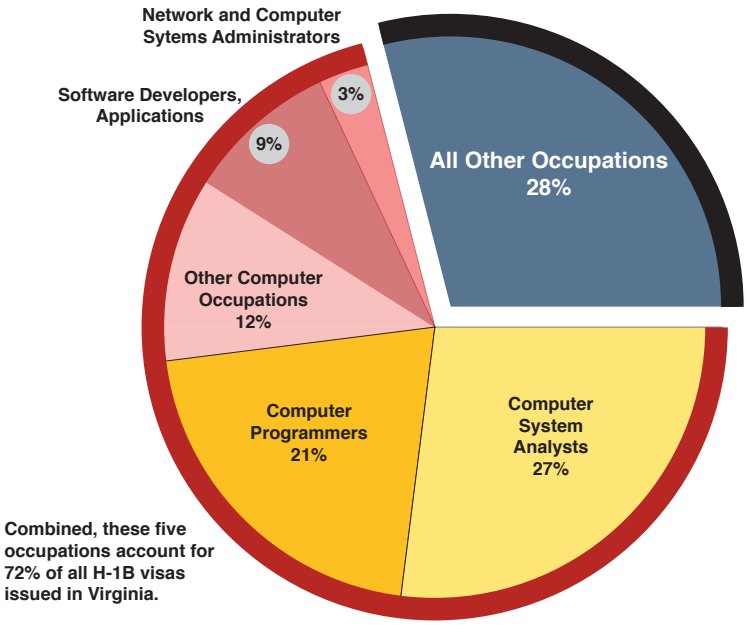
The commonwealth is third nationally in computer systems design and related services jobs, employing 142,600; is fifth in employing engineering services; and third in computing systems design and related services jobs (fig. 1).

Figure 1: Current and Projected Employment in Cybersecurity in Virginia



Source: Virginia Employment Commission and U.S. Bureau of Labor Statistics, 2012-2022

Figure 2: Percentage of Employment-based (H-1B) Visas Issued in Virginia by Occupation



Source: U.S. Department of Labor, Office of Foreign Labor Certification. (2013). Annual Report October 1, 2012–September 30, 2013. Retrieved from http://www.foreignlaborcert.doleta.gov/pdf/OFLC-2013_Annual_Report.pdf

As the need for cybersecurity jobs increases and the gap in filling those jobs remains, employers look to workers from other countries. While security clearances may limit the range of positions attained by individuals with H-1B nonimmigrant visas—the employment-based, non-immigration visas granted to individuals with highly specialized knowledge—Virginia is depending on workers from other countries to help close the workforce gap in computer and networking jobs. Seventy-two percent of the occupations in which persons with H-1B visas are employed are in computer-related fields (fig. 2).

In 2014, 19.3 percent of Virginia's payroll came from technology companies. Technology industry workers' wages are more than double that of other private-sector workers' wages, and Virginia is the fifth highest state in technology payrolls—$29.3 billion (CompTIA Properties LLC, 2015). At its core, cybersecurity includes jobs to develop secure software to enhance security and jobs related to providing security and monitoring systems.

With a high need for trained people to fill these positions, it is not surprising that cybersecurity jobs pay well (fig. 3). There are many levels of jobs, so pay varies based on job descriptions and education levels or certifications required. As an example, cybersecurity engineers average $75,299 at Raytheon and $150,606 at Booz Allen; cybersecurity analysts average $59,929 in the U.S. Air Force and $106,777 at Lockheed Martin (Glassdoor, 2015). There are many job titles and categories of work in cybersecurity (e.g., intrusion analyst, incident responder, malware analyst, and security auditor), making it difficult to predict salary ranges.

Consider one position advertised by the National Security Agency in June 2015. The position, exploitation analyst, evaluates target opportunities and strategizes activities

Figure 3: Earnings and Growth for Selected Occupations in Virginia

Atmospheric and Space Scientists	
Median Wages, Virginia (2013)	$106,010
Employment Estimate (2012)	433
Annual Job Openings	32
Biomedical Engineers	
Median Wages, Virginia (2013)	$90,200
Employment Estimate (2012)	456
Annual Job Openings	26
Compliance Officers	
Median Wages, Virginia (2013)	$64,270
Employment Estimate (2012)	6,852
Annual Job Openings	203
Computer and Information Systems Managers	
Median Wages, Virginia (2013)	$141,830
Employment Estimate (2012)	16,732
Annual Job Openings	577
Database Administrators	
Median Wages, Virginia (2013)	$91,580
Employment Estimate (2012)	6,215
Annual Job Openings	273
Logisticians	
Median Wages, Virginia (2013)	$80,350
Employment Estimate (2012)	6,675
Annual Job Openings	264
Information Security Analysts	
Median Wages, Virginia (2013)	$103,840
Employment Estimate (2012)	10,025
Annual Job Openings	662
Telecommunications Equipment Installers and Repairers	
Median Wages, Virginia (2013)	$56,620
Employment Estimate (2012)	4,908
Annual Job Openings	105

Source: Virginia Employment Commission and U.S. Bureau of Labor Statistics, 2012-2022.

against particular networks. The salary ranges from $64,923 to $96,931. The requirements for the position can be a combination of education and experience: high school diploma and eight years of experience, or an associate degree and seven years of experience, or a bachelor's degree and five years of experience, continuing on to a doctoral degree and no experience.

While a long list of technical degrees, certifications, and training are included with the job announcement, the qualification options demonstrate the flexibility employers have to fill positions. This explicit flexibility serves as evidence that a trained workforce is unavailable to fill all of the positions open.

Supplying Education and Training

THE FEDERAL CALL FOR MORE EDUCATION

Attention to cybersecurity education has been growing at the federal level since January 2008 when President George W. Bush launched the Comprehensive National Cybersecurity Initiative (CNCI). The following year, President Barack Obama conducted a review of security issues and efforts and implemented 12 strategies in support of CNCI (See https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative). One of those strategies addresses the importance of expanding cyber education:

> "While billions of dollars are being spent on new technologies to secure the U.S. government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950s, to meet this challenge."

In addition to CNCI, the National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort to advance education and training opportunities for cybersecurity career preparation. NICE is coordinated by the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce.

NICE defines the work within the cybersecurity field to help maintain a globally competitive cybersecurity workforce and broaden the pool of skilled workers capable of supporting a cyber-secure nation. It includes federal departments and agencies, industries, and academic institutions beginning with K-12 (http://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education). NICE has 13 Virginia affiliates, including seven educational institutions: George Mason University, Hampton University, James Madison University, Marymount University, Norfolk State University, Northern Virginia Community College, and Virginia Tech.

NICE works in four arenas to strengthen cybersecurity education: (1) national awareness, (2) formal education, (3) workforce structure, and (4) workforce training and professional development. This work aims to achieve three outcomes:

1. **Enhance Awareness** about and access to cybersecurity issues and resources; improve citizens' knowledge to allow them to make smart choices as they manage cyberspace risks; and, improve knowledge of cybersecurity within organizations so that resources are well applied to meet the most obvious and serious threats.

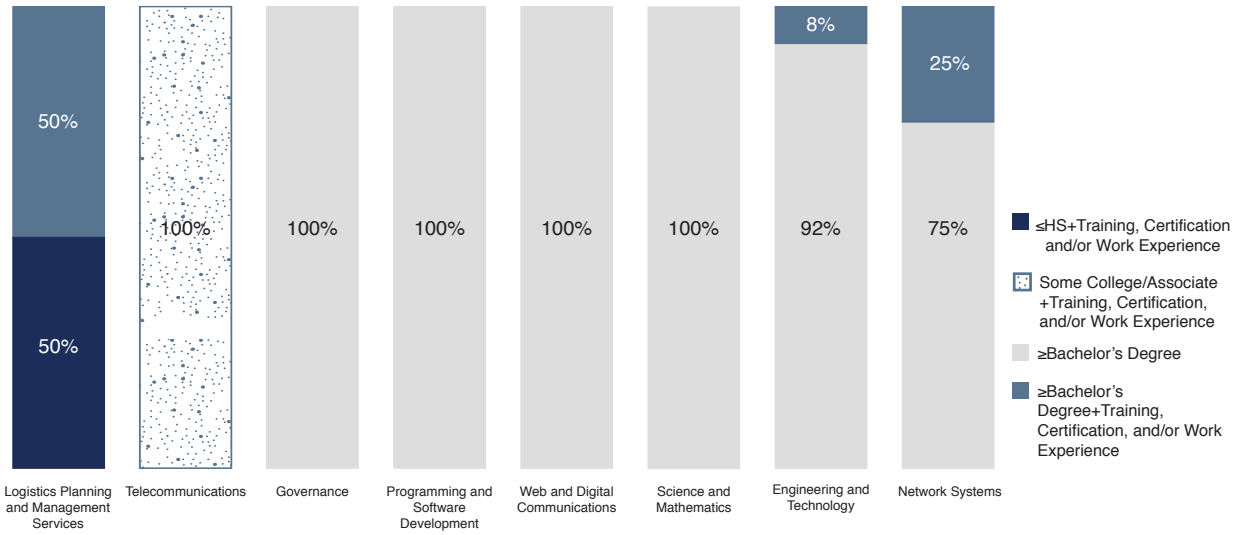
2. **Expand the Pipeline** to strengthen the academic pipeline leading to cybersecurity careers. The National Science Foundation and the U.S. Department of Education lead this effort, which is the formal cybersecurity education component of the initiative.

3. **Evolve the Field** to increase the quality and quantity of the cybersecurity workforce by determining the merits of professionalization; delivering a recommended method to help organizations better forecast their cybersecurity workforce needs; developing a strategy to recruit and retain a cybersecurity workforce for the nation; and establishing standards and strategies for cybersecurity training and professional development. This component is led by the Homeland Security, Defense, and Labor departments.

HOW TO BUILD QUALIFICATIONS FOR CYBERSECURITY CAREERS

Career-specific education for cybersecurity jobs currently begins at the postsecondary level and includes opportunities to attain knowledge, skills, and attributes that match jobs in a variety of ways (i.e., some jobs require only a workforce credential, while others require a college degree and several credentials).

Figure 4: Predominant Education Level for Cybersecurity



Source: Virginia Employment Commission and U.S. Bureau of Labor Statistics, 2012-2022.
NOTE: Trailblazers created these education categories based on education information included with U.S. Bureau of Labor Statistics 2012-2022 employment projections files which differs from "typical education needed for entry" assigned to each occupation by Bureau of Labor Statistics.

Steps to cybersecurity jobs in Virginia include (fig. 4):

- Workforce credentials – career studies certificates and exam-based certifications
- General education leading to an associate degree
- Bachelor's degree
- Graduate degrees (master's or doctorate)
- Continuing education

These experiences are enhanced with opportunities for internships, apprenticeships, and competitive events, which are becoming available or being discussed by companies, but they require corporate or government support. Security clearances and access to proprietary information can be a barrier to establishing internships or other training opportunities.

The Council on Cybersecurity reports that the industry looks for the following in job candidates, beyond required education levels (Council on CyberSecurity, 2015):

1. Hands-on skills and hands-on experience
2. Matching certifications to the job role
3. Performance competitions
4. Formal training as an indicator of interest and commitment
5. An assessment of the provider of training

With a large number of job descriptions and a variety of companies seeking these workers, there is no one path to a particular job. Job seekers will be most successful if they can demonstrate their qualifications in three areas: (1) education beyond high school, (2) certification in specialized skills related to cybersecurity, and (3) experience that confirms workforce or soft skills. Additionally, some jobs require a security clearance. The development of a pathway to cybersecurity careers may be better understood by examining how existing institutions provide the education and training needed to develop qualifications for a range of jobs.

Universities: According to the Bureau of Labor Statistics, Virginia ranks first in the nation in the percentage of computer systems analysts and computer software engineers in the workforce. Virginia's universities produce more than 2,150 technology graduates annually. These graduates are the product of 14 university programs that offer certifications or a degree in cybersecurity. Virginia Commonwealth University offers a cybersecurity degree. The following universities offer certifications in cybersecurity:

- James Madison University
- Longwood University
- Marymount University
- Old Dominion University
- Radford University
- University of Mary Washington

Table 1: Enhancing Opportunities for Cybersecurity Careers at Virginia Colleges and Universities

College/University	Degree Offered	Certification Available	National Security Agency Accredited	Enrichment Activities
George Mason University	✓		✓	
James Madison University		✓	✓	Boot camp for high school teachers
Longwood University	✓	✓		
Marymount University		✓	✓	
Mary Washington University	✓	✓		
Norfolk State University	✓		✓	Department of Energy-funded K-12 activities
Old Dominion University	✓	✓		
Radford University		✓		Course for Grades 6-12
University of Richmond	✓			
University of Virginia		✓		
Virginia Commonwealth University	✓			
Virginia State University		✓		
Virginia Tech		✓	✓	Offers federal CyberCorps Scholarship for Service; hosted 2015 U.S. Eastern Cyber Challenge and Cybersecurity Camp for high school students
Hampton University	✓		✓	
Community Colleges* Danville Germanna John Tyler Lord Fairfax Piedmont Thomas Nelson Tidewater Virginia Western	Associate		✓ Northern Virginia and Lord Fairfax *Thomas Nelson is pursuing accreditation.	Thomas Nelson Community College offers summer boot camp for security professionals. Northern Virginia Community College offers associate degree and a security certificate transferrable to four-year colleges.

*17 of the 23 Virginia community colleges offer one or more courses aligned to cybersecurity.

- University of Virginia
- Virginia State University (offers a minor)
- Virginia Tech

The National Security Agency (NSA) National Center for Academic Excellence in Cyber Defense Education has accredited the following cybersecurity programs in Virginia:

- George Mason University: 2014-2021
- James Madison University: 2014-2020
- Marymount University: 2014-2020
- Norfolk State University: 2014-2020

George Mason University and Virginia Tech are accredited as NSA National Centers for Academic Excellence in Cyber Defense Research, 2014-2021.

As Virginia universities have contributed to preparing the workforce by offering various degrees associated with cybersecurity/information technology, they also support activities to enhance traditional course offerings with competitions, challenges, and student scholarship programs. For example:

- Norfolk State leads a $25 million effort that begins with kindergarten activities in an effort to develop cybersecurity professionals. Funded by the Department of Energy, Norfolk State is leading a consortium of Historically Black Colleges and Universities, a school division, and the Department of Energy National Laboratories to develop STEM education that will lead to security careers.
- Virginia Tech participates in the Federal CyberCorps Scholarship for Service program, which provides full tuition and up to $25,000 per year in scholarships to students interested in pursuing careers in cybersecurity. The program is open to students majoring in computer science or computer engineering.
- James Madison University hosted a cybersecurity boot camp for high school teachers during the summer to raise awareness and encourage the integration of cybersecurity topics into the curriculum.
- Virginia Tech hosted the 2015 U.S. Cyber Challenge and Cybersecurity Camp for high school students in the eastern United States. This competition seeks to recruit 10,000 of America's brightest students to usher into next generation cybersecurity professional jobs.

Community Colleges: Postsecondary education is required for most security-related jobs. Seventeen of Virginia's 23 community colleges offer one or more courses aligned to cybersecurity. Eight community colleges offer security certificates. These programs are determined locally and can contribute to building a career pathway throughout the commonwealth. About 600 students complete associate degrees in cyber or IT categories each year in Virginia.

Community colleges provide opportunities for continuing education for those already in

security jobs. As one example, Thomas Nelson Community College offered a summer boot camp to prepare practicing security professionals for a leading industry security certification, Certified Information Systems Security Professional (CISSP).

Responding to workforce needs in Northern Virginia, Northern Virginia Community College (NVCC) offers an associate of applied science (AAS) degree and career studies certificate in cybersecurity. The AAS is transferable to four-year colleges and designed to provide the knowledge, skills, and abilities of the comprehensive NICE National Security Workforce Framework. NVCC's career studies certificate in cybersecurity is designed to provide expertise in security for networking specialists and prepares students for two certification exams that are required for some cybersecurity jobs.

NVCC has been accredited as a NSA National Center for Academic Excellence in Cyber Defense in Two-Year Colleges, 2014-2020. Both Lord Fairfax and Thomas Nelson community colleges are pursing this accreditation.

"Strong career paths for middle and high school students provide not only cyber awareness but opportunities for them to explore the plethora of career and job options available as they continue their education. At Northrop Grumman we provide opportunities for high school and college students to work as interns and learn first-hand from seasoned professionals what it is like to work in the cybersecurity area and the impact of those efforts."

Ray Kinard
Director,
Northrop Grumman Cyber Academy,
Northrop Grumman Corporation

Certifications: Cybersecurity offers many professional certifications that help workers obtain jobs and continue training as needs increase. The National Initiative for Cybersecurity Careers and Studies (NICCS), an affiliate of the Department of Homeland Security, serves as a national resource for government, industry, academia, and the public to learn about cybersecurity awareness, education, careers, and workforce development opportunities. NICCS has identified 15 organizations that provide professional cybersecurity certifications needed in the career field. These organizations offer a hierarchy of certifications that address many job titles within domains such as cryptography, risk and analysis, and network and communications security. One of the 15 organizations, Cisco, certifies within six categories: entry, specialist, associate, professional, international expert, and architect. NICCS provides a listing of all the cybersecurity or cybersecurity-related education and training courses offered in the United States. Currently, there are more than 1,300 courses available. Virginia's community colleges as well as national proprietary institutions are among the institutions providing access to these courses.

Cybersecurity is associated with computer science, but the far-reaching impact of cybersecurity touches many career areas, including public policy and business. Students preparing to work in the cybersecurity field may find value in an interdisciplinary approach to their education, because cybersecurity specialists will continue to be needed to protect all phases of infrastructure. In the future, cybersecurity may become a formalized discipline. Until that time, current programs of study and certifications offered by Virginia's community colleges and universities as well as proprietary schools can provide a basis for designing a

career pathway that should begin with career and technical education programs in middle grades and high schools.

Workforce Skills: Many of the workforce or soft skills shared across career clusters are required for success in the cybersecurity field. The ability to solve problems, work in teams, find creative solutions, and communicate to external groups has been a workforce priority for several decades.

The report of the 2013 National Roundtable on Security Talent Development emphasizes the importance of experiential learning and critical thinking in the preparation of potential talent (Apollo Education Group, 2013). Companies not only value these skills in their workers but also look for people who have the attributes needed to project into the future and invent solutions to problems that have yet to be identified. Ninety percent of the 300 defense contractors and government agencies participating in a 2015 workforce study said that possessing communication skills is viewed as the most important contribution to a successful security professional (Frost & Sullivan, 2015).

> The importance of soft skills was emphasized at the 2015 National STEM Forum on Security Risks and Emerging Workforce Solutions. Representatives from the cybersecurity community suggested the importance of these skills and sent this message to the education community:
>
> *"We're looking for people with a lot of breadth, workers who can deal with complex problems and drill down."*
>
> *"I can teach someone to code but I can't teach them how to think outside the box."*
>
> *"Hybrid skills – someone who can write and hold a conversation across legal, finance, and HR."*
>
> *"You want folks who can speak to people at all levels. Communications as a skill set is important."*
>
> *"The only way to defend is to play around and do the 'what ifs.' We're looking for a team of out-of-the-box thinkers."*

CURRICULUM AND INSTRUCTIONAL RESOURCES FOR K-12 INSTRUCTION

Aside from federal resources, there are limited curricular and instructional resources for K-12 that can guide career pathway development. Cyber professionals have suggested that security courses should be integrated with other areas of education to develop a full set of skills needed in these jobs. One path to integrating cybersecurity into programs in states and schools is to include cybersecurity in STEM programs, academies, or curricula. In fact, one of the objectives of NICE is to ensure that this occurs. Although STEM programming in K-12 has been publicized and encouraged for many years, STEM is not yet a priority in most school curricula and is viewed by some as an add-on. But STEM resources are abundant, and STEM curriculum and other classroom supports may offer an opportunity to integrate cybersecurity with STEM programs or provide a model for developing cybersecurity materials. This is an initial step to increase awareness about cybersecurity for students in STEM programs, but other strategies will be needed to begin addressing the immediate

workforce development needs.

The following examples of cybersecurity programs and resources include K-12 efforts. They represent a range of initiatives occurring throughout the nation to introduce cybersecurity education: integrating units of study, adopting a special curriculum, developing career and technical courses and career pathways, providing online services, and offering workshops and camps. While these initiatives have not been vetted as best practices, the resources included below are promising practices in cybersecurity education, and they can inform the curriculum and instructional decisions posed when creating a new career pathway.

Virginia's Cyber Security and Cyber Forensics Infusion Units**:** In Virginia, school divisions have taken the first step to integrate cybersecurity into the career and technical education curriculum by implementing cybersecurity lessons that can augment existing course materials. Cyber Security and Cyber Forensics Infusion units are available for instruction in any program. This material includes the following:

- Eighty-five (85) tasks/competencies that can be incorporated into any existing course.
- **Correlation between the tasks/competencies and Virginia Standards of Learning** (SOL) for English, History and Social Science, Mathematics, and Science.
- **Computer/Technology Standards of Learning** for grades 6-8 and 9-12 that align to knowledge, skills, and attributes in cybersecurity. Included are Basic Operations and Concepts; Social and Ethical Issues; Technology Research Tools; Thinking Skills, Problem Solving, and Decision Making; Technology Communication Tools; and Leadership Development Expectations (at grades 9-12).
- **Information on three additional cybersecurity units** that are part of the Cyber Explorations Pilot Program, a collaboration between Longwood University, the Longwood Center for Cyber Security, Hanover County Public Schools, Superior Document Services, community mentors, and experts from around the globe.
- **Two Governor's STEM academies –** Marshall Governor's STEM Academy and Chantilly Governor's STEM Academy, both in Fairfax County, have developed cybersecurity camps and implemented them during the summer months.

NICE Strategic Plan – Cybersecurity in K-12 Formal Education**:** NICE is focusing on two strategies to increase the pool of skilled workers capable of supporting a cyber-secure nation. The first objective is an Early Focus on STEM Curriculum by emphasizing the important role of mathematics and computational thinking beginning in elementary grades. The second objective is to increase the quantity and quality of academic computer science courses in high schools. Actions to accomplish these objectives include the following:

- aligning federal cybersecurity education budgets with the NICE plan;
- assisting private entities that produce computer science and cybersecurity instructional materials, tools, and resources for K-12 STEM instruction;
- assisting corporations and foundations to organize around formal computer science education efforts at the state level;

- helping the cybersecurity workforce partner with schools to provide expertise and role models to students; and
- providing access to curriculum and assessments for courses in CTE and a proposed Advanced Placement course, Computer Science Principles.

The National Integrated Cyber Education Research Center (NICERC), created by the Cyber Innovation Center (CIC)**:** NICERC was created by CIC to advance its academic outreach and workforce development program in Louisiana. The impact of NICERC is the creation of a "Cyber Interstate" that provides multiple opportunities for students to become aware of cyber issues (enhance awareness), engage in cyber education (expand the pipeline), and select cyber careers (evolve the field). Supported with federal funding to scale its work nationally to grow cyber education, NICERC focuses on curriculum design, professional development, and collaboration in K-12 education.

NICERC works with its partners to design project-driven, application-based curricula that engage students across elementary, secondary, and postsecondary levels. The curricula provide school systems with a rigorous program that showcases a systems-level understanding of real-world applications of STEM. Professional development incorporates liberal arts components, which allows teachers to embed the curricula across multiple disciplines to prepare students to become the next generation of engineers and cyber professionals.

NICERC is working with seven state departments of education to build cyber pathways that prepare students to meet the growing demand for cyber professionals and the 21st century workforce. Teachers from 39 states are accessing the NICERC curricula for their classrooms. Virginia's Pulaski County Public Schools is using NICERC resources to plan cybersecurity education that begins in middle school science classrooms and continues through the Governor's STEM Academy.

Maryland Department of Education, Office of Career and Technology Education**:** Maryland, Virginia, and the District of Columbia comprise the geographical region of fast-growing cybersecurity jobs referred to as the Cyber Corridor, so it may be helpful to understand how this neighboring state is viewing cybersecurity in CTE. Maryland CTE has located its cybersecurity program in the Human Resource Services Cluster and Homeland Security Pathway of the state's career program offerings.

Maryland's Homeland Security and Emergency Preparedness (HS/EP) Program is a career and technical education instructional program that integrates government, academia, and private sector training/educational initiatives to help students understand how the United States and its interests worldwide are protected against threats to public safety, both natural and manmade, through effective communication, preparedness, detection, prevention, response, and recovery.

The program offers three career strands:

- Homeland Security Sciences
- Criminal Justice/Law Enforcement

- Information/Communications Technology

These three strands align with the six mission areas of the U.S. Department of Homeland Security:

- Intelligence and Warning
- Protection of Critical Infrastructure and Key Assets
- Border and Transportation Security
- Domestic Counterterrorism
- Defense Against Catastrophic Threats
- Emergency Preparedness and Response

In this program, students are expected to:

- Outline the essential characteristics of national and international acts of terrorism.
- Classify the roles, functions, and interdependency between local, federal, and international law enforcement, intelligence, and military agencies.
- Develop effective strategies to generate information necessary for intelligence and law enforcement organization agency heads to make timely, effective, and efficient decisions on the directions and methods of Homeland Security policies and operations.
- Examine the global and national issues and policies concerning terrorism and Homeland Security.
- Employ technology for general and critical legal research, writing, and case management.
- Demonstrate proficiency in communication, problem solving, and team building skills.
- Explain and justify the ethical standards needed for careers in the Health and Human Services Cluster.
- Participate in internship experiences that include exposure to multiple career areas within the chosen program strand.
- Explore career opportunities within the Human Resource Services Cluster and Homeland Security Pathway.

> *"We have $190,000,000 [worth of] reasons to have cybersecurity curriculum at the high school level. That is the current Virginia Income Tax going uncollected due to approximately 40,000 cybersecurity jobs unfilled in Virginia."*
>
> **Michael Miklich**
> **Chief Executive Officer,**
> **Cybersecurity Education Inc.,**
> **STEM/CTE Cybersecurity Education**

National CyberWatch Center K-12, supported by the National Science Foundation**:** This center offers comprehensive resources for development, pilot, and delivery of K-12 cybersecurity content and programs at the elementary, middle, and high school levels. It is routinely sought out to assist with curriculum and development of programs across the country.

Programs are offered before, during, and after school, including summers. Signature events include an annual conference in Cyberethics, Cybersafety and CyberSecurity Awareness, training for counselors in cyber careers, and an annual Cool Careers in Cyber Security

for Girls Workshop. This center supports career and technical education with a formal CyberSecurity High School Career Pathway; SECURE IT: Strategies to Encourage Careers in CyberSecurity and IT; and CyberROOTS: Cyber-Ready for Opportunities and Occupations in Tech Security. The Center's formal CTE Cyber Security Program of Study is approved by the Maryland State Department of Education.

iFORCE – Institute for Cybersecurity Education**:** iFORCE offers a secondary educational program to prepare students for the skills and certifications needed to be qualified for Department of Defense jobs. The Institute provides highly technical coursework that students can take as electives throughout their secondary education, grades 9-12. iFORCE's 10 courses prepare students for specific certification exams through the four years of study.

The courses that comprise the cybersecurity pathway are as follows:

- Computer Systems Technology (freshman year) – Certifications: CompTIA A+ and Testout PC Pro
- Computer Network Software Operations (sophomore year) – Certifications: CompTIA Network+ and Testout Network Pro
- Comp TIA Security+ (sophomore year) – Certifications: CompTIA Security+, ISC^2 SCCP, and Testout Security Pro
- Programming C++ (junior year)
- Programming Java (junior year)
- Advanced Computer Network Software Operations "Windows" (junior year) – Certifications: Microsoft 70-680 & 687, Testout's Windows Client Pro, and Microsoft (MS 70-410) Windows Server Pro: Install & Configure
- Advanced Computer Network Software Operations "Linux" (senior year) – Certification: CompTIA Linux+
- Senior Project/Internship and Advanced Programming
- Advanced Programming – Python (senior year) – Portfolio of programs developed
- Advanced Programming – EC – Council Certified Ethical Hacker (senior year) – Certification: EC – Council C EH v8 Certification

Air Force Association CyberCamps**:** In the summer of 2015, the first Air Force Association (AFA) cybersecurity camps were conducted in 22 locations across the nation. Virginia's Battlefield High School, in Prince William County, and Chantilly Governor's STEM Academy and Marshall Governor's STEM Academy in Fairfax County, hosted three of the one-week camps. AFA CyberCamps were created to supplement the CyberPatriot's annual National Youth Cyber Defense Competition, which engages students in cybersecurity education throughout the year. The program office recommends that camps recruit students in grades 7-12 with no prior education in cybersecurity.

Through the standard AFA CyberCamp program, schools and educational organizations can order a curriculum kit consisting of instructional modules, instructor's guides, student workbooks, demonstration software, and competition software that will teach skills in cyber safety and cybersecurity. CyberCamp kits can be requested by public and private high

schools and middle schools as well as other specified groups. The 20-hour curriculum is designed to be conducted over five days.

StaySafeOnline**:** The National Cybersecurity Alliance's mission is to educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individual's use, the networks they connect to, and our shared digital assets. NCSA provides this online safety resource that teachers can access for grades K-2, 3-5, middle and high school, and higher education. The site has lessons, tips, and information pages that cover an extensive amount of content related to cybersecurity in an appealing format.

This online program begins with basic information about social media use from which young students and parents can benefit. StaySafe provides flexibility to schools or individual teachers who are beginning to incorporate cybersecurity into the regular curriculum. StaySafe is broad enough to be helpful when matching cyber studies with existing career studies.

Hacker Highschool Project (HHH) – Security Awareness for Teens (hackerhighschool.org and www.secom.org): The nonprofit ISECOM researches and produces the Hacker Highschool Project as a series of workbooks to help teens become better hackers, better students, and better people. Hacking is taught as a skill used through many types of businesses in a positive way. HHH reflects a concern that teens are in a world with major communication and productivity channels open to them, and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them as they use the Internet. HHH offers lessons on utilizing Internet resources safely, such as Web privacy, chat, mobile computing, and social networks. Each HHS lesson is designed as self-contained learning and no teacher is required. This program has been accessed around the globe.

Developing a Course Framework

Efforts to address the cybersecurity workforce needs have primarily rested with postsecondary education. As information technology (IT) has been closely associated with computer science, long considered a subject reserved for postsecondary education, it is not surprising that college degrees and industry certifications required for cybersecurity careers have been the responsibility of colleges, universities, and proprietary schools and not included in K-12 career readiness programs. However, with the increasing need to fill jobs with qualified applicants, it is appropriate for career and technical education in public schools to extend the existing "infusion units" to an explicit career pathway designed to develop the knowledge, skills, and attributes needed for cybersecurity professionals while encouraging students to pursue these important careers.

> *"Bringing the cybersecurity discussion into the classroom can be the spark that leads some students to seek out more advanced education, training and certifications on their way to careers in cybersecurity."*
>
> **Rick Geritz**
> **Chief Executive Officer,**
> **LifeJourney,**
> **Online STEM Education**

Virginia is developing a cybersecurity pathway to be implemented in middle grades and high schools. As teams are established to begin this important work, it is beneficial to examine resources developed by state or educational groups, which provide cybersecurity resources and materials that can inform the standards, framework, and competencies upon which the pathway and subsequent courses will be designed.

STANDARDS AND COMPETENCIES

Career and technical education develops career pathways that are based on validated standards and job-based competencies. A rigorous process is followed to ensure that the standards upon which the program is based and the competencies that are used to define courses are aligned to the needs of the workplace.

Currently, there is no single set of standards for a cybersecurity program that is (1) designed for middle and high school students, (2) cooperatively developed to align with postsecondary programs in cybersecurity, and (3) fluid enough to address current and emerging workplace needs. This gap is not surprising given the lack of cybersecurity programming at the secondary level and the relatively young cybersecurity industry. If standards are to be found that help direct a career pathway, the STEM areas – science, technology, engineering, and mathematics – may be helpful, recognizing that cybersecurity is not limited to the technological aspect of the work and may be integrated with other Career Clusters it serves.

At the 2013 National Roundtable on Security Talent Development, participants noted a lack of standardization of the many courses and certifications available throughout the country.

They emphasized that "additional educational standards and certifications, particularly at the entry level, would help the security industry meet organizational standards and attract a well-qualified workforce" (Apollo Education Group, 2013). The 2013 Roundtable report recommends ensuring that curriculum and competency standards for security training apply to a variety of job descriptions, and that standards focus on interdisciplinary and integrated programs.

The Computer Science Teachers Association's (CSTA) K-12 Computer Science Standards can help inform cybersecurity development in career and technnical education because both cyber safety and cybersecurity are deeply embedded in these science standards (CSTA, 2015). The standards are presented in three levels: Level 1 for Grades K-6, Level 2 for Grades 6-9, and Level 3 for Grades 9-12. Levels 1 and 2 contain learning standards focusing primarily on cyber safety, while Level 3 contains learning standards for cybersecurity. Cybersecurity topics at Level 3 fall under one of three headings:

- Computer Science in the Modern World,
- Computer Science Concepts and Practices, and
- Topics in Computer Science.

At each of the three levels standards are organized by strands: computational thinking; collaboration; computing practice; computers and communication devices; and community, global, and ethical impacts. (See http://csta.acm.org/Curriculum/sub/K12Standards.html.)

ORGANIZING PRINCIPLES

Cybersecurity jobs may be viewed under two particular organizing principles, or frameworks, developed by government agencies and collaborators. Each of these products is the result of the contributions of many individuals associated with building a cybersecurity workforce, and both are relevant to career pathways under development.

A **National Cybersecurity Framework** was developed in response to President Obama's Executive Order, "Improving Critical Infrastructure Cybersecurity," in 2013. The framework consists of three parts: Framework Core, Framework Profile, and Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and references that are common across critical infrastructure sectors. The Framework enables organizations to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. Twenty-two categories of work (e.g., protective technology, analysis, governance, and communications) are grouped by one of five functions: Identify, Protect, Detect, Respond, and Recover (National Institute of Standards and Technology, 2014). This framework includes a glossary and list of acronyms related to cybersecurity that can be helpful as novices investigate security resources and prioritize information for a career pathway.

The National Institute for Cybersecurity Careers and Studies offers a second framework, the interactive National Cybersecurity Workforce Framework, on its Web site that may be helpful to alternate paths to a career. (See http://niccs.us-cert.gov/training/national-cybersecurity-workforce-framework.) The framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas:

1. Securely Provision
2. Analyze
3. Operate and Maintain
4. Oversight and Development
5. Collect and Operate
6. Protect and Defend
7. Investigate

In addition to this framework, NICCS provides a list of competencies or areas of expertise required for successful performance of a job function. The Web site provides the types of workforce characteristics – knowledge, skills, and attributes – an individual must exhibit for each competency. NICCS's 30 competency areas include a range of expertise including computer forensics, computer skills, criminal law, encryption, human factors, and infrastructure design.

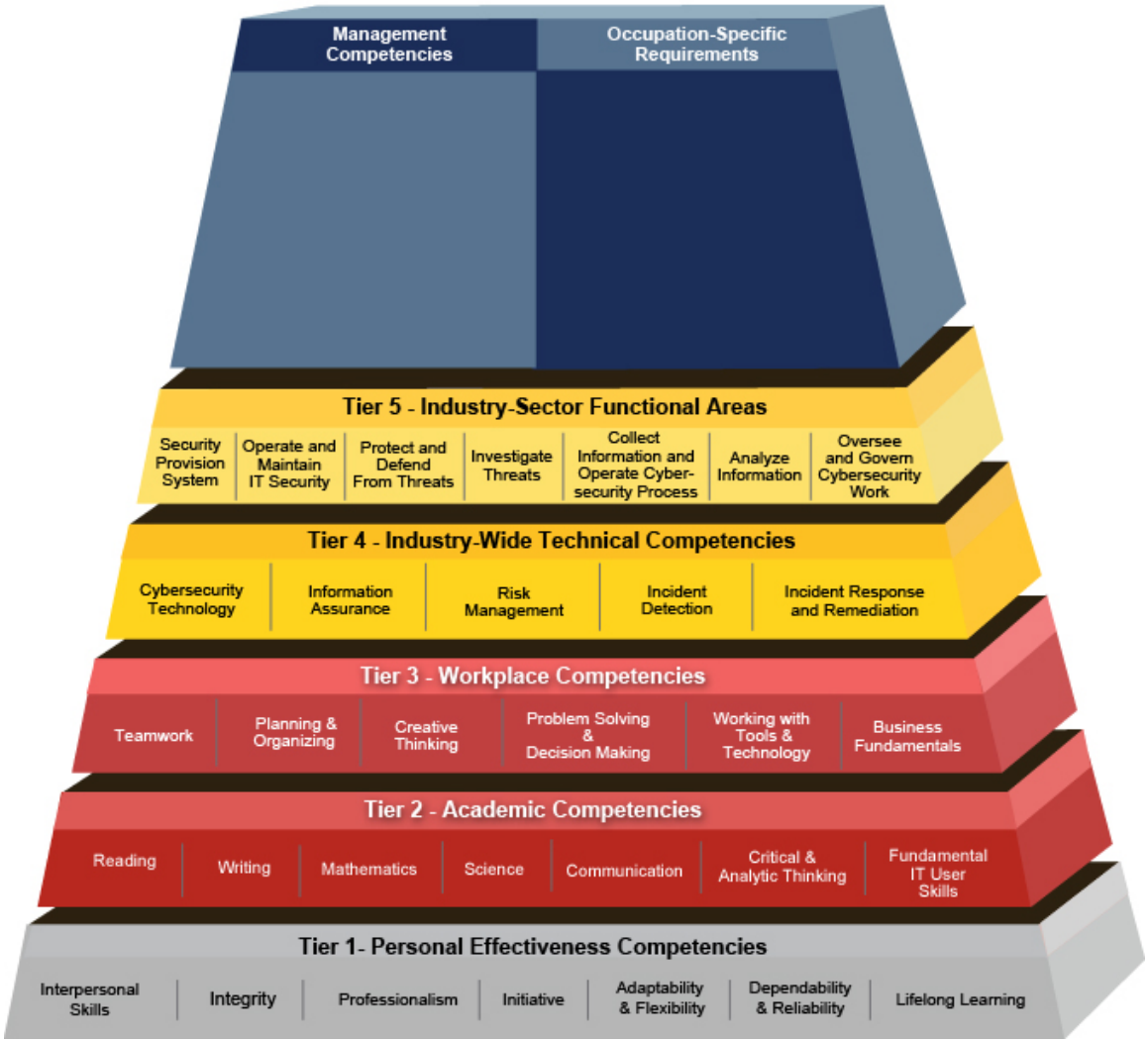
Virginia has adopted the National Cybersecurity Workforce Framework through the work of the Virginia Cyber Security Commission.

MODEL

In support of NICCS's National Cybersecurity Workforce Framework, NICE and its partners have developed a comprehensive competency model of cybersecurity. This interactive Web-based model, called the Cybersecurity Competency Model, helps to describe NICCS's Framework.

The Cybersecurity Competency Model incorporates the competencies identified in the framework and complements the framework by including both the competencies needed by trained cybersecurity professionals and those needed by workers from most any career whose job routinely requires use of the Internet.

Cybersecurity Competency Model



Source: Competency Model Clearinghouse, http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx.

Taking Immediate Action

Based upon a national review of calls to action, current and developing programs, and materials for cybersecurity education summarized in this paper, additional follow-up is recommended. The following action steps are suggested to initiate discussions that will lead to the work plan. These action steps are not prioritized, presented in any recommended sequence, or necessarily dependent on other actions.

1 INCREASE KNOWLEDGE

Develop a working knowledge of what cybersecurity is and the careers and jobs that are associated with cybersecurity/information technology. Become familiar with cyber-related vocabulary, standards, and work-related competencies that will be important in workgroup discussions.

- Identify the Career Cluster(s) under which the pathway will best serve Virginia's needs.
- Generate a list of credentials that will be complementary to the career pathway or program of studies in cybersecurity.
- Collaborate with business and industry representatives who have expressed an interest in cybersecurity workforce development.
- Correlate the Workplace Readiness Skills for the Commonwealth to the cybersecurity program.
- Review the CSTA K-12 Computer Science Standards to inform a scope and sequence of cybersecurity topics.
- Align the cybersecurity course to the Virginia Standards of Learning (SOL). The Virginia Cyber Security and Cyber Forensics Infusion Unit's correlation to Standards of Learning is a starting point.
- Examine the National Cybersecurity Workforce Framework to identify competencies associated with job functions.

2 REVIEW CURRENT PRACTICES

Identify the most relevant cyber education initiatives occurring in or around Virginia that may contribute in some way to the pathway development.

- Become knowledgeable of the range of cybersecurity education and training opportunities available through federal agencies, including the Department of Defense, National Security Agency, and Department of Homeland Security (e.g., Stokes Educational Scholarship Program for computer science majors; CyberCorps Scholarship for Service; and internships, fellowships, and training to expose students to national security mission).

- Consider how student competitive events in cybersecurity, which are valued by employers, can be included in the program developed for the pathway.
- Develop a plan for preparing K-12 school counselors to develop expertise in cybersecurity training and education, scholarships and financial support, and career opportunities.
- Develop a working knowledge of cybersecurity-related courses in Virginia's community colleges and identify which colleges will be prepared to offer dual enrollment courses in this area.
- Identify the type of middle grades initiatives that focus on career exploration and awareness for cybersecurity and connections to STEM activities that would strengthen the career pathway.
- Invite postsecondary schools to share information about their cybersecurity federal initiatives.
- Learn more about the cybersecurity career pathways implemented in Maryland and Louisiana, especially noting any lessons learned that can guide Virginia's development process.
- Meet with Virginia's community colleges to understand the dual enrollment opportunities.
- Review information on all of the curriculum and instructional resources described in this paper.

3 SECURE TALENT

Name a variety of education, corporate, business, and government representatives to share information associated with developing the pathway.

- Identify state and federal government representatives who bring unique expertise to discussions about career opportunities and competencies required for successful employment.
- Include certification test developers or testing providers as deemed necessary. (They may best serve as resources to be called upon as needed.)
- Include representatives from security companies that are the primary employers for the pathway. Representation should include new start-ups as well as established government contractors.
- Invite one or more of Virginia's universities that has received recognition for its vision to promote cybersecurity.
- Name local career and technical education and STEM Academy directors who have integrated cyber education into existing career and technical education courses.

4 IDENTIFY RESOURCES

Develop a manageable list of resources that can inform the development of the pathway.

- Acquire the glossary and list of acronyms related to cybersecurity that are published in the 2013 National Cybersecurity Framework.
- Become familiar with all components of the Cybersecurity Competency Model.
- Become familiar with NICCS's National Cybersecurity Workforce Framework.
- Review current and recent National Science Foundation grant awards in Virginia with a cybersecurity component that could enhance the development of the pathway.
- Evaluate resources needed to market cybersecurity education, including job opportunities in Virginia and how trends in technology impact the growing need for a cybersecurity workforce.
- Learn more about NICE from one of Virginia's affiliates.
- Solicit information from the National CyberWatch Center K-12 as a potential partner in the development of the pathway.

Works Cited

Apollo Education Group. (2013). *Enterprise Security Risks and Workforce Competencies: Findings from an Industry Roundtable on Security Talent Development.* University of Phoenix.

Center for Strategic International Studies. (2010). *A Human Capital Crisis in Cybersecurity, Technical Proficiency Matters.*

CompTIA Properties LLC. (2015, February 9). *2015 Cyberstates.* Retrieved 2015, from https://www.comptia.org

Council on CyberSecurity. (2015, June 15). *Developing the Cybersecurity Workforce.* Retrieved June15 2015, from Council on CyberSecurity: www.counciloncybersecurity.org/workforce/

Cragle, F. R. (2015, August 3). *The Importance of Comprehensive Cyber Insurance*. Retrieved August 13, 2015, from Virginia Business: www.virginiabusiness.com/opinion/article/the-importance-of-comprehensive-cyber-insurance

CSTA. (2015, April 8). *Cybersecurity, Cybersafety and the K-12 Computer Science National Standards*. Retrieved from http://csta.acm.org/Advocacy_Outreach/Other/CSTACyberStandards.pdf

Elazari, K. (2015, April). How to survive cyberwar. *Scientific American, 312*(4), 66-69.

Frost & Sullivan. (2015, April 16). *The 2015 (ISC)2 Global Information Security Workforce Study.* Retrieved August 12, 2015, from GISWC: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Glassdoor. (2015, July 22). *Cybersecurity Salaries*. Retrieved August 12, 2015, from Glassdoor: http://www.glassdoor.com/Salaries/cyber-security-salary-SRCH_KO0,14_IP2.htm

Marsan, C. D. (n.d.). *Hottest IT Skill? Cybersecurity.* Retrieved March 26, 2015, from Network World: www.networkworld.com/article/2188242/malware-cybercrime/hottest-it-skill--cybersecurity.html

Mashable. (2015, August 18). *All of the Cyberattacks on the U.S. Government (That We Know of).* Retrieved September 1, 2015, from Mashable.

National Institute of Standards and Technology. (2014, February 12). Framework for Improving Critical Infrastructure Cybersecurity.

NY Times. (2015, February 5). *9 Recent Cyberattacks Against Big Businesses.* Retrieved September 1, 2015, from The New York Times: http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html

Revere Digital LLC. (2015, April 20). *Raytheon to Buy Cyber Security Firm Websense in $1.9 Billion Deal.* Retrieved April 21, 2015, from re/code: http://recode.net/2015/04/20/raytheon-to-buy-cyber-security-firm-websense-in-1-9-billion-deal/

Riley, W. (2014, October 27). *Cyber Attacks on U.S. Companies in 2014.* Retrieved September 1, 2015, from The Heritage Foundation: www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

Scribner, B. (2015, March 24). Building the Nation's Cybersecurity Workforce. *Changes, Challenges, and Collaborations: Effective Cybersecurity Training.* Gaithersburg, MD: Federal Information Systems Security Educators' Association.

STEMconnector. (2015, April 14). Emerging Strategies and Solutions in Cyber Security. *National STEM Forum on Security Risks and Emerging Workforce Solutions*. Washington, DC.

Symantec. (April 2015). *ISTR20 Internet Security Threat Report.*

Viveras, M. (2013). *Cybersecurity Education for the Next Generation: Advancing a Collaborative Approach.* IBM Center for Applied Insights. Armonk, NY: IBM Corporation.

For more information about CTE programs, visit the CTE Resource Center's Web site.