WEST VIRGINIA CYBERSECURITY

WORKFORCE STRATEGIC INITIATIVE REPORT

JANUARY 2019

OPPORTUNITY:

WEST VIRGINIA MUST INVEST NOW TO EXPAND

ITS CYBERSECURITY LEARNING OPPORTUNITIES

– AT ALL LEVELS. BY DOING SO THE MOUNTAIN STATE

WILL CREATE A LARGER TRAINED CYBER WORKFORCE,

ENHANCE ITS ECONOMIC DIVERSIFICATION AND

BE IN A MORE COMPETITIVE POSITION TO CAPITALIZE

ON EMERGING TECH EMPLOYMENT OPPORTUNITIES.

CONTENTS

WV CYBERSECURITY WORKFORCE STRATEGIC INITIATIVE REPORT 5-45

LIST OF PARTICIPANTS ON W.VA. CYBERSECURITY WORKFORCE STRATEGIC PLANNING GROUP 47-49

W.VA. DEPARTMENT OF EDUCATION CYBER EDUCATION PLAN 50-55

NGA REPORT ON STATE CYBER WORKFORCE INITIATIVES 56-62

THANK YOU TO OUR PARTNERS
FOR THEIR COMMITMENT TO THIS PROJECT.

HIGH TECHNOLOGY FOUNDATION℠

TECHCONNECT
WEST VIRGINIA

WEST VIRGINIA
FORWARD

TECHCONNECT
WEST VIRGINIA

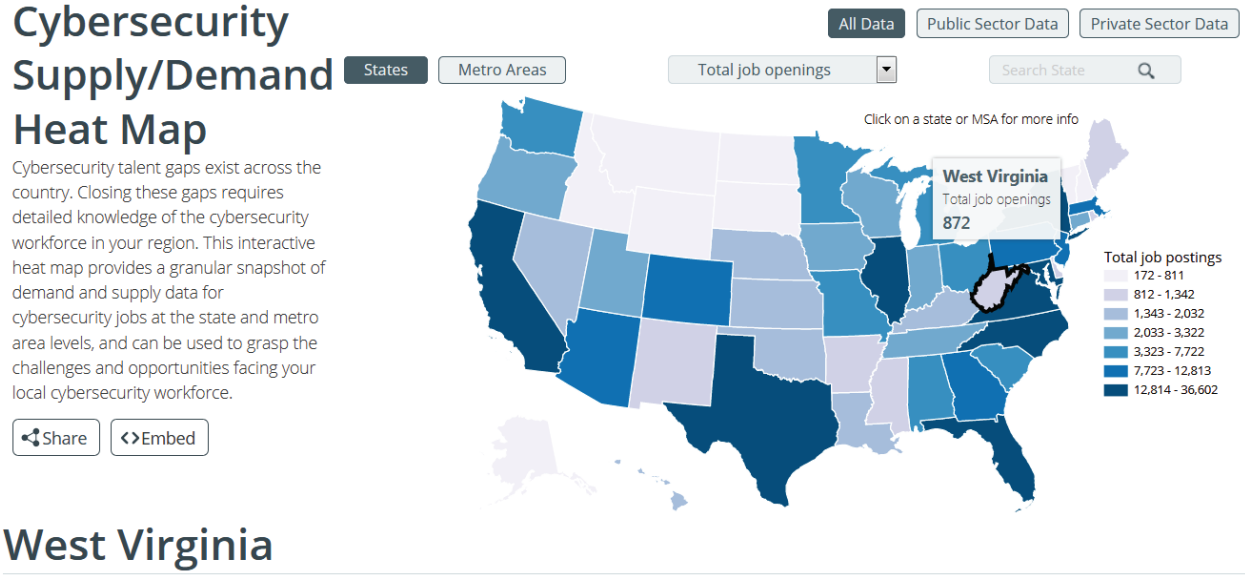
West Virginia Cybersecurity Workforce Strategic Initiative Report

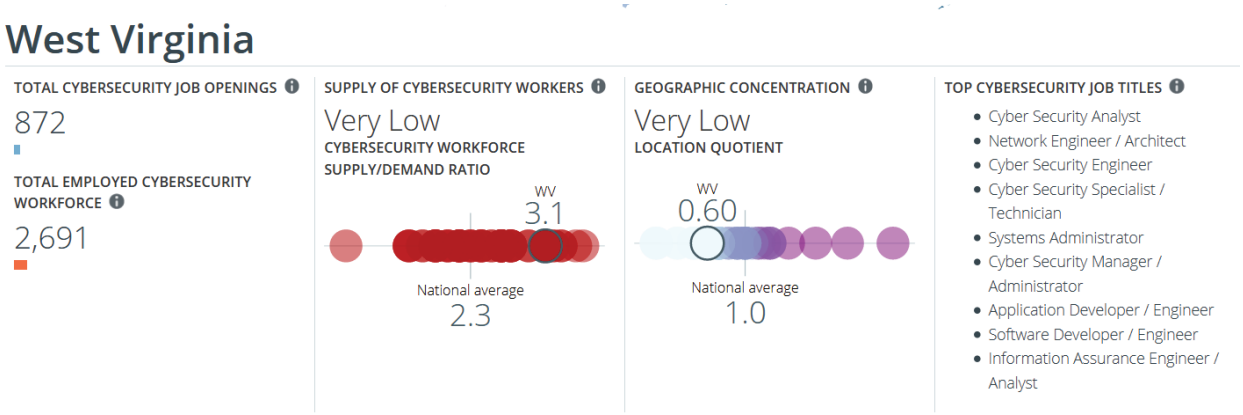
TechConnect West Virginia has been the driving force behind the West Virginia Cybersecurity Workforce Strategic Initiative. TCWV is a non-profit coalition committed to the advancement of the innovation economy in West Virginia, focused on four technology sectors: advanced energy, chemicals and advanced materials, biosciences, and biometrics. With broad representation from private industry, the public sector, and higher education, TechConnectWV seeks to diversify the state's economy, promote economic prosperity and create high-paying jobs.

Among other key partners supporting this initiative are the West Virginia Office of Technology, the W.Va. High Technology Consortium, the West Virginia National Guard and West Virginia Forward.

1. Opportunity

Job opportunities for cybersecurity professionals are growing significantly, but a large percentage is going unfilled within the United States (and the world), particularly within the military and the federal government -- national and homeland security as well as intelligence (Rand, 2014). Such unfilled positions complicate securing the nation's networks and may leave the United States ill-prepared to carry out conflict in cyberspace. And, this cyber shortage also poses dangers to critical infrastructure, our health care and banking systems, to governments of all sizes and to business large and small. According to cyberseek.org (2018) in West Virginia (WV) there are currently 872 cybersecurity job openings with a total employed cybersecurity workforce of 2,691. At the national level there are 313,735 total cybersecurity job openings with a total employed cybersecurity workforce of 715,715.





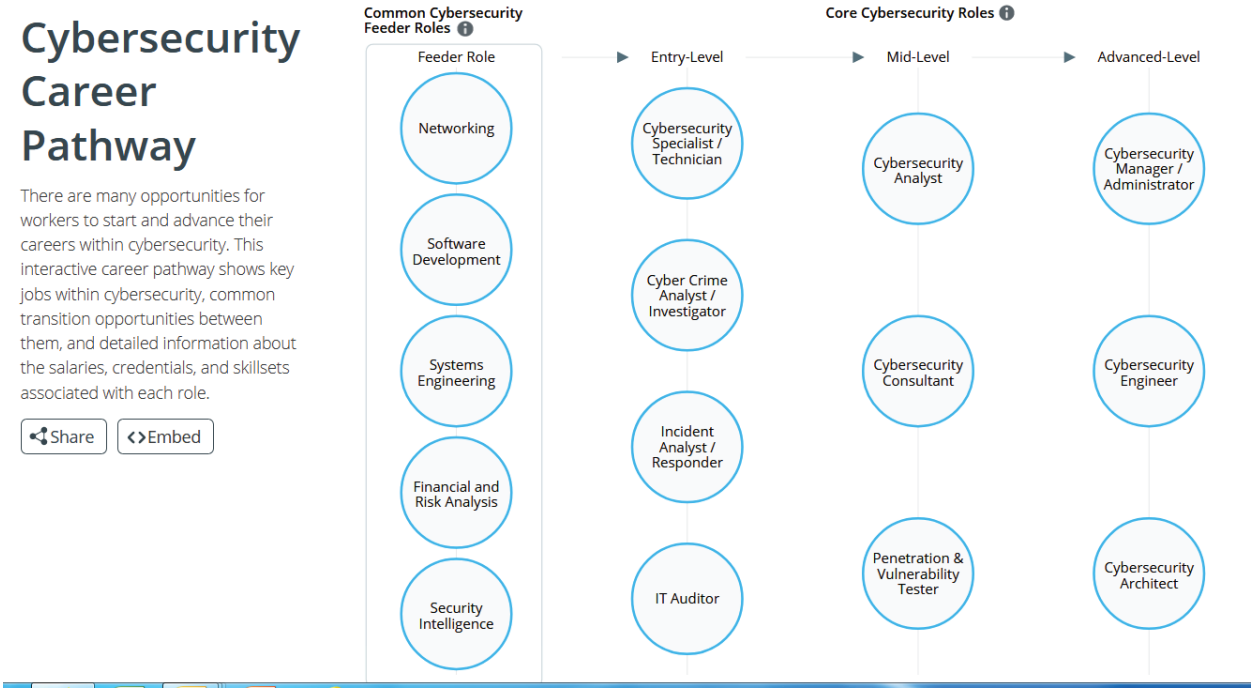
These numbers will increase because, according to the Department of Labor's Bureau of Labor Statistics, the field of cybersecurity is projected to grow at a rate of 28% from present to 2026. Other reports indicate that the need for cybersecurity works is approaching staggering numbers:

- B**y 2022 there will be a need for 1.8 million more professionals in the cybersecurity field,** according to a 2017 report from the Center for Cyber Safety and Education™ (the Center) — part of its eighth Global Information Security Workforce Study (GISWS) - sponsored by (ISC)²® and Booz Allen Hamilton. https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/02/13/Cybersecurity-Workforce-Shortage-Continues-to-Grow-Worldwide

- Another report puts this **cyber workforce need at 3.5 million by 2021**: https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

- **NICE Workforce Demand fact sheet** https://www.nist.gov/sites/default/files/documents/2017/11/16/workforce_demand_111617_final.pdf

However, more and more positions continue to go unfilled because employers cannot find candidates with the correct skills. Here is an outline of cyber career pathway: (*Source: https://www.cyberseek.org/pathway.html*)



West Virginia must invest now to expand its cybersecurity learning opportunities – at all levels. By doing so the Mountain State will create a larger trained cyber workforce, enhance its economic diversification and be in a more competitive position to capitalize on these emerging tech employment opportunities.

2. Overview

Mission

To develop a strategic plan on how to accelerate cybersecurity education in both K-12 and higher education.

Objectives

1) Align interested agencies, institutions, businesses and stakeholders in a focus on cybersecurity workforce training and employment opportunities
2) Seek input and recommendations from cybersecurity businesses and specialists
3) Analyze and make recommendations on workforce training programs across the educational attainment continuum
    a. High school
    b. Two-year
    c. Four-year
    d. Certificate
4) Review policies and projects in other states (Virginia, Michigan)
5) Develop strategies on workforce development and economic opportunities related to cybersecurity…share with Governor Justice in the fall of 2018.

Action Items

- Compile an overview of the existing cybersecurity degrees provided in West Virginia (WVU, Marshall, FSU, UC, AB, C&TCs)…and new programs (WVU, Marshall) being developed.
    - Share this info with key state leaders and key policymakers

- Provide analysis to the WVSBDC on its cyber assessment on-line tool and promote tech firms to add their cyber services to the WVSBDC.

- Have cyber employers evaluate the current cybersecurity curriculum and degrees provided by the community & technical colleges -- BridgeValley, Pierpont, Blue Ridge, Northern.

- Explore the development of cyber internship programs with employers – large and small.

- Work with the W.Va. Dept. of Education to provide recommendations on cybersecurity learning courses and STEM applications for middle and high school students. The CyberPatriot high school program provides useful curricula components for incorporation into classroom learning.

- Help recruit more cyber specialists to be "tech experts" to grow youth cyber programs/activities (CyberPatriot, GirlsGoCyberStart, etc.) at more high schools in the state.

- Prepare an overview of the key resource needs facing the existing cybersecurity degree programs at four-year institutions, particularly related to the high costs associated with cyber software needed for classroom instruction.

- Work with existing federal agencies (NOAA, NASA, U.S. Dept. of Commerce, etc.) and contractors in WV to understand their cybersecurity workforce needs.

- Develop an integrated cybersecurity workforce plan of action.

- Outline a new web site that will provide information on high-tech training programs, curriculum and degrees in the areas of cybersecurity (and maybe coding).
    - Seek a volunteer web/back-end developer

Findings

Provided are key cyber job domains that the work group identified:

Security and Risk Management.
Asset Security.
Security Engineering.
Communications & Network Security.
Identity & Access Management.
Security Assessment & Testing.
Security Operations.
Software Development Security.

https://resources.infosecinstitute.com/the-cissp-domains-an-overview/

Provided are cyber industry certifications that the group identified:

- Industry
  - Certified Information Systems Auditor (CISA)
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Ethical Hacker
- DoD 8570
  - CompTIA Security+ certification
  - ISC2 CAP certification
- NIST - https://niccs.us-cert.gov/training/search/itsm-solutions-llc/nist-cybersecurity-framework-foundation-certification-training
  - Cyber Operations
  - Training, Education and Awareness
- Other
  - CompTIA Security+
  - GSEC: SANS GIAC Security Essentials

Working Groups

As part of this group's deliberations, subgroups were developed to analyze key cybersecurity educational strategies and make recommendations on the workgroup's ongoing focus areas:

1) Cybersecurity Career Pathway/Training Program
    - Work with the state education leaders to analyze and provide recommendations on an integrated career pathway in cybersecurity and relevant course offerings
        - High School (W.Va. Dept. of Education)
        - Community & Technical College (one-year, two-year)
        - Four-year programs (University of Charleston, Marshall, WVU, Fairmont State, etc.)
        - Online learning options
        - Model? - http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cyber-courses-2017.pdf
    - Develop informational resources to share with students so they understand other non-education factors for those interested in pursuing careers in cybersecurity
        - Credit history
        - Personal activities
        - Criminal record
        - Soft-skills
    - Develop a speaker forum of cyber specialists who could meet with students.
    - Explore the expansion or introduction of cyber STEM activities
        - CyberPatriot program (currently being introduced in WV)
        - Build cyber programs off of the state's successful WV Robotics Alliance
2) Real-World Experience/Private-Sector Needs
    - Outline needs and unique issues (clearances) of different employers as it relates to cyber workforce:
        - Government agencies, contractors
        - Financial industry
        - Health care industry
        - Private-sector cyber services providers
    - Evaluate benefits of generalist (mile wide, inch deep) vs. specialist?
    - Develop course curriculum recommendations to develop a baseline cyber education program
        - Explore "certificate" programs in WV
    - Examine new ideas to reduce employment barriers related to clearances
        - State cyber incentive program (to cover the costs of security clearances)
    - Review existing industry-recognized cybersecurity credentials
    - Develop a state cyber internship program and other policy matters
    - Develop a Cyber Civilian Corps program (modeled after Michigan's)
3) Recruitment/Outreach
    - Develop a strategic campaign (and resources) to recruit cyber specialists/security clearance individuals back to WV
    - Enact state legislation to provide tax relief to cyber specialist who return to WV
        - Military retirees
    - Develop an outreach and education campaign to encourage cyber education/training and promote job opportunities among interested West Virginians of all ages
4) Long-Range Strategy
    - Interconnect with the state Office of Technology on its cyber strategic objectives
    - Study model programs in other states
5) Military
    - Develop a plan of action on how to leverage and recruit WV National Guards people, veterans and military retirees who have cyber skills or who could be trained.

3. Cyber Workforce Team Members

A multi-disciplinary team of cyber experts, employers, government officials and educators from across West Virginia has assembled as part of this strategic planning process. Those members include representatives from higher education, government, private industry, tech firms, technology-related organizations and the military.

See Appendix A for a complete list of the workforce team members.

4. Situational Overview

According to McKinley & Company, every year, hackers produce some 120 million new variants of malware. Several billion data sets are breached. And companies report thousands of attacks every month, ranging from the trivial to the extremely serious. Think WannaCry, NotPetya, Meltdown, and Spectre. And, these statistics do not include cyber incidents from within companies or agencies.

In December 2016 the Information Systems Security Association (ISSA) and analyst firm Enterprise Strategy Group (ESC) published a report from a survey of cyber security professionals worldwide that concluded that current staff lack the skills to properly defend networks. The study found: “Some 54% of organizations in the study have suffered at least one security event in the past year, and most attribute the events to a lack of security staff or training. Some 70% of organizations report the cybersecurity skills gap has had an impact on them.

Among the reasons for these security failures: the cybersecurity team isn't big enough (31%); insufficient training for non-technical employees (26%); cybersecurity isn't a high priority for business, and executive management (21%). Nearly 55% say their existing cybersecurity teams are facing heavy workloads given the lack of manpower available such that 35% do not have enough education and training in their security tools to successfully fulfill their jobs. "One of the things leading to some breaches is in fact some lack of cybersecurity talent," says Jon Oltsik, Enterprise Strategy Group. "To me, this is an existential threat that changes our strategy on what we have to do in cybersecurity." The survey findings also indicated that security pros feel they don't have adequate time or resources for training to keep up with new threats and defenses.” "

Presidential Executive Order

To respond to this critical workforce shortage, President Trump issued an Executive Order in the fall of 2017 that directs the U.S. Secretary of Commerce, in conjunction with the Secretary of Homeland Security and in consultation with other Federal Departments and Agencies, to assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future. This includes cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education. The order also calls for a report to the President with findings and recommendations regarding how to support the growth and sustainment of the Nation's cybersecurity workforce in the public and private sectors.
https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

Articles

The articles and links listed below provide additional information about the workforce needs in the cybersecurity field.

Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens
(ISC)² CYBERSECURITY WORKFORCE STUDY, 2018
https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx
This link summarizes a cyber workforce study done by (ISC). While there are no major revelations in the study, there is some interesting data on education:

- The least important factor in the "Qualifications for Employment (pg.9) was "Cybersecurity or related undergraduate degree."
- Additionally, 34% reported having a Masters and 39% having a Bachelors, with an average of 13 years in IT, and 7 years on cybersecurity initiatives.

Unraveling the Cyber Skills Gap & Talent Shortage
https://www.cybrary.it/2018/03/unraveling-cyber-skills-gap-talent-shortage/

Three Ideas for Solving the Cybersecurity Skills Gap
One possibility: Create a Cybersecurity Peace Corps
https://www.wsj.com/articles/three-ideas-for-solving-the-cybersecurity-skills-gap-1537322520

Boosting the Cyberworkforce
Amid persistent shortages in cybersecurity positions, what can states do to strengthen their numbers? *http://www.govtech.com/data/Boosting-the-Cyberworkforce.html?mc_cid=6056097651&mc_eid=629541aaa5*

Cybersecurity Workforce Development: A Primer
https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-workforce-development/

Cybersecurity could be WV's next big growth area, leaders say
http://wvmetronews.com/2017/08/05/cybersecurity-could-be-wvs-next-big-growth-area-leaders-say/
Why Cyber Security Degrees Are Becoming Increasingly Valuable
http://everydayconsumer.org/why-cyber-security-degrees-are-becoming-increasingly-valuable?articleid=1059&&utm_campaign=1410658&utm_medium=msn-defaulthomepage&utm_source=300192

5. Cyber Threats

Cyber threats facing the United States come from several primary sources: international governments, criminal elements and individual hackers. And, generally, these take the forms of the following:

- Industrial IoT Hacks
- Ransomware
- Phishing
- Internal threats, data thefts
- Denial of service

"Connected devices are essential to our professional and personal lives, and criminals have gravitated to these platforms as well. Many common crimes—like theft, fraud, harassment, and abuse—are now carried out online, using new technologies and tactics. Others, like cyber intrusions and attacks on critical infrastructure, have emerged as our dependence on connected systems revealed new vulnerabilities. Successfully mitigating these threats relies on a combination of information sharing, prevention efforts, and enforcement work. Government agencies, law enforcement, the private sector, and individuals all have a role to play."
Source: FBI, https://www.fbi.gov/news/stories/ncsam-2018

The threats and costs associated with cybersecurity crimes are increasing and becoming more and more complex. It is projected that cyber crime damage costs are projected to hit $6 trillion annually by 2021.

Source: Top 5 cybersecurity facts, figures and statistics for 2018
Predictions and observations provide a 30,000-foot view of the cybersecurity industry
https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

6. Cyber Employment and Economic Opportunities in West Virginia

Cybersecurity jobs exist in West Virginia, and many of these jobs are clustered in a few areas:

- Northcentral West Virginia (Harrison, Marion and Monongalia Counties)
  - Federal agencies including the FBI, NASA, NOAA, NETL and the U.S. Dept. of Commerce
  - Businesses such as Northrop Grumman, Leidos, ManTech, General Dynamics IT, IBS Corporation, Fusion Technology, XO Security, Sevatec and Critical Solutions
- Rocket Center (Mineral County)
  - IBM
  - Northrop Grumman
- Eastern Panhandle (Berkeley and Jefferson Counties)
  - Coast Guard
  - Office of Personnel Management

In addition, a variety of cybersecurity jobs are embedded in hospitals, banks, local governments and in state government.

In early 2019 there will be an effort made to better quantify these jobs and to highlight those employers in West Virginia who have cybersecurity jobs and openings.

7. Cyber Learning Opportunities in West Virginia

There are a variety of learning opportunities in West Virginia for those interested in cybersecurity. These opportunities begin in high school and progress to a Master's level.

Five four-year institutions of higher learning in West Virginia currently provide cybersecurity degrees:

1. Alderson Broaddus University
2. Fairmont State University
3. Marshall University
4. University of Charleston
5. West Virginia University

Two other institutions are developing new cyber programs. Bethany College is developing a new B.S. in Cybersecurity, and Bluefield State University is planning to offer a minor in cybersecurity.

Cyber education overviews from each are provided below. These also include information on how the institutions are working to provide "hands on" learning experiences and skills.

Alderson Broaddus University

1. An overview of your institution's cybersecurity offerings and specialties

Alderson Broaddus University started a new higher education program on cyber security in Fall 2018. The program is firmly grounded in the computer science and engineering discipline, with extensive opportunities for hands-on practical and industry level applications. The program offers a number of academic degrees that provide student teachings in a broad range of knowledge areas through a rich, robust, and industry-focused cybersecurity curriculum.

AB's cybersecurity program is created with a vision to ensure the provisioning of fundamental knowledge and practical hands-on experience that comprise the major areas of cyber security science. This vision is emphasized in the program design, academic plans, and curricular considerations. The curricula of AB's cybersecurity programs are structured based on the academic requirements of the NSA DHS National Centers of Academic Excellence in Cyber Defense. All coursework related to computer science is structured based on the IEEE/ACM 2013 standards for computer science programs.

Through a firm engagement with cybersecurity industry, Alderson Broaddus University assures the consideration of the contemporary domain challenges and the latest cyberspace technology in the program teachings. A board of university industry alliance advisory provides informed guidance to the cybersecurity program on the campus and shares expertise and knowledge by reviewing program curriculum, facilities, equipment, budget, etc.

The main goal of AB's cybersecurity program is to produce skilled professionals with practical cyber defense expertise strengthened by computing and information technology skillsets. The program will prepare AB's students for the multi-disciplinary aspects of securing software, networks, web and mobile systems. Through different program terms and specializations, AB's degree programs provide options for students to pursue careers of interests in both general and industry-specific cybersecurity domains.

Program Mission and learning outcomes

The mission of the Cyber Security program at Alderson Broaddus University is to provide a Bachelor of Science degree in Cyber Security consistent with the university mission that prepares students to protect against attackers and malicious activities, design secure software systems, assure information security, and understand professional, ethical and legal responsibilities.

The program enables students to attain the following goals by the time of graduation.

1. Use and apply knowledge of computing and mathematics appropriate to the discipline.
2. Apply knowledge of cyber security to protect against attackers and malicious activities.
3. Design and develop secure software systems.
4. Protect against network threats and internet hijacks.
5. Assure information security and implement secure system access control.
6. Design security methods and secure algorithms using cypher communication.
7. Demonstrate professional, ethical, legal, security and social issues and responsibilities.
8. Utilize advanced security techniques in the fields of digital forensics, healthcare informatics, or cyber security management.
9. Use current techniques, skills, and tools necessary for security practices.

Degree Programs:

Bachelor of Science degree in Cyber Security

The BS degree in cybersecurity is a four-year program with three concentrations on digital forensics, healthcare security, and cybersecurity management. In its main stream, the BS degree will prepare students in a broad range of cyberspace disciplines including secure software, networks security, web and mobile system security. The program provides students with the required knowledge and skillsets to take strong leadership roles in protecting organizations' information infrastructures and mobilize appropriate resources to maintain stable operations. In addition to the broad knowledge about the state-of-the-art methods and techniques of cybersecurity, students will be equipped with the required knowledge base and expertise to foster new security solutions to defend against cyber-attacks and all types of malicious activities. Further capacities and tactics will be focused on in this program including the capabilities to combat hacking, intrusion, and other cyber threats and to assure information system's secure access and to construct new cryptographic methods and secure algorithms in cypher communication. Moreover, students will be acquainted with the existing software vulnerabilities and the methodologies to design and development secure software systems and consider the suitable countermeasures in these systems with respect to the prevention of, detection of, reaction against, and recovering from cyber-attacks. Furthermore, they will be able to guide and prepare organizations to the compliance with the latest cybersecurity standards.

Through a set of elective courses, the students will extend their learning with the knowledge about valuating technology assets and the risks of cyber threats associated with them. It also enriches their intellect with the methodologies to critically analyze an organization's risk profile, implement a suitable risk mitigation strategy, and protect from unauthorized disclosure, modification, or withholding of information resources. Through the program's elective courses, the students will be exposed to the latest tools and resources for monitoring and defending cyber activities. Other cybersecurity management skills include the capabilities to analyze network traffic and identify malicious activities at the communication and application levels. Students will be able to apply their learnings on digital forensics to investigate computing scenes, detect security breaches, and assure containment. They will be also capable of conducting forensic analysis methods at multiple high- and low-level technology tiers including application, system, software, network, and communication. They will also be equipped with ethical computer hackings tactics to conduct digital forensic activities by following the fundamental principles and legal considerations. Further concentration will be on healthcare security. The healthcare security concentration will prepare students to take an effective role in securing healthcare informatics by extending their learning to the specific features and security requirements of medical organizations. Understanding the nature of medical and clinical data, as well as the ethical and privacy concerns of this data is a vital goal of this concentration. Students will also be acquainted with basic knowledge about the main activities in the healthcare process, the major technology resources of medical organizations, and the fundamental security techniques to secure the healthcare

activities of these organizations. This knowledge will also enable the student's capabilities to perform cyber risk analysis and security management activities of medical organizations.

Minor degree in Cyber security

The minor degree in cybersecurity allows students in other disciplines (e.g., computer science and business administration) to supplement their major degrees with basic cybersecurity skills. In addition to improving their professional expertise and career plans, these students will be prepared to take effective cybersecurity roles in their specific domains. Students in these programs will learn the basic knowledge of cybersecurity and the broad aspects of cyber threats and security countermeasures. They will focus their cybersecurity learning on network and internet security in addition to the underlying knowledge about computer science and computer networks.

Associate degree in Cyber security

The associate degree in cybersecurity is a two-year program that allows students to start their career path earlier by focusing their learning on core cybersecurity knowledge areas appropriate to most employers. Then, these graduates can pursue further education, training, or certification tracks according to their employer needs. Students in this program will learn the basic knowledge of cybersecurity and the broad aspects of cyber threats and security countermeasures. They will focus their cybersecurity learning on network, internet, and software security in addition to the underlying knowledge about computer science, software design, computer architecture, and computer networks.

2. Ensuring the provisioning of hands-on experiences with the latest tools and technology

The cyber security program at Alderson Broaddus University is created with a vision to ensure the provisioning of practical hands-on experience. This vision is emphasized in the program design aspects as follows:

- **Program design philosophy**

  At AB, we believe that native and robust cyber security solutions are mostly implemented at the low level of computing and engineering domains. Thus, our cybersecurity program will produce skilled professionals with practical cyber defense expertise strengthened by computing and information technology skillsets.

- **Curriculum design**

  The curricula of our cybersecurity programs are structured based on the academic requirements of the NSA/DHS National Centers of Academic Excellence in Cyber Defense.

- **Program scope**

  Our Cyber Security program prepares students in a broad range of cyberspace disciplines including secure software, networks security, web and mobile security, information and system security, cyber risk management, ethical hacking, digital forensics, security operation technology, in addition to system administration, cryptography, software and system programming, database systems, and others.

- **Program learning outcomes**

  The program provides broad knowledge about the state-of-the-art methods and techniques of cybersecurity. Students will be equipped with the required knowledge base and expertise to foster new security solutions to defend against cyber-attacks and all types of malicious activities. Further capacities and tactics will be focused in this program including the capabilities to combat hacking, intrusion, and other cyber threats and to assure information system's secure access and to construct new cryptographic methods and secure algorithms in cypher communication.

- **Lab work in program courses**

Since most of the program courses are practical and require hands-on skills, the courses are designed to include extra 1-credit hour of lab work. Labs are designed based on the state-of-the-art techniques as well as the ongoing needs of industry.

- **Industry Alliance**

Through a firm engagement with cybersecurity industry, AB assures the consideration of the contemporary domain challenges and the latest cyberspace technology in the program teachings. A board of university-industry alliance advisory provides informed guidance to the cyber security program on the campus and shares expertise and knowledge by reviewing program curricula, facilities, equipment, budget, etc. The Industry alliance board also assists in locating needed resources and help strengthens the program graduates' quality and improve their employment opportunities, among several other responsibilities.

- **Concentrations**

Through different program terms and specializations, our degree programs provide options for students to pursue careers of interests in both general and industry-specific cybersecurity domains. Through a set of elective courses, students will be able to extend their learning in special knowledge areas, namely, digital forensics, healthcare security, and cybersecurity management.

Fairmont State University

The Center of Excellence (COE) for Cyber at Fairmont State University (Fairmont State) provides the leadership and best practices necessary for the cyber-related challenges of tomorrow. The Center is a collaboration among multiple disciplines throughout the University allowing it to be more efficient and effective at providing the next generation workforce to the world. The Center is that logical grouping of disciplines that in isolation provide value-added disciplined scientists, engineers and managers, etc. In order to combat tomorrow's challenges however, industry and government cannot rely on disciplined/isolated solutions. A holistic solution is needed to solve tomorrow's cyber-related challenges, an integrated capability, in which we can leverage the strengths from each of the specialized disciplines to produce the highest quality graduates armed with a breadth of knowledge, skills, and capabilities.

The COE for Cyber has integrated the University's capabilities related to the Cyber-disciplines to ensure the curriculums are relevant, practical experiential learning, state-of-the-art, and produce the highest quality graduates. The Center includes the disciplines of computer science, cyber security, national security and intelligence, information systems management, and robotics. Integrating these capabilities into a Center of Excellence enables the University to be more efficient with its resources while increasing the quality of education and services it provides not only to its students but to its customers across industry and government.

Fairmont State University Capabilities:

Computer Science with a Concentration in Cybersecurity

The Bachelors of Science Degree in Computer Science with a concentration in Cybersecurity at Fairmont State offers extensive hand-on experience through the incorporation of rigorous laboratory sections and/or coding projects in all the main cybersecurity courses.

In Fundamentals of Computer Security, students acquire hands-on laboratory experience starting the second week and continuing on a bi weekly basis throughout the semester. In the lab, students learn how to navigate the Linux command line, OpenSSL encryption, crack passwords using Kali Linux, manipulate Linux environment variables

and file permissions like set-UID, and perform the BASH exploit Shellshock. Students also learn about secure application coding by implementing a buffer overflow attack in C.

In Cryptography, students learn to implement encryption and decryption algorithms in C++, starting with ancient Roman ciphers and progressing through modern ciphers including the symmetric DES and AES ciphers and the asymmetric RSA encryption algorithm.

In Network Security, students learn basic networking and fundamental principles of network security as well as intermediate network attacks and countermeasures. In the separate lab section, students explore tracking cookies, examine and implement C code for packet sniffing and constructing raw packets, use the Linux netwox toolkit and built-in Kali Linux tools to perform and counter ARP poisoning, Denial of Service attacks, and TCP session breaking and hijacking for remote code injection. Students learn networking security principles by hands on configuration exercises with Cisco wireless routers, Cisco adaptive security appliances, and Linux firewalls and application proxies.

In Vulnerability Assessment, the Cybersecurity capstone course, students learn to analyze computer system vulnerabilities by working through a variety of actual and theoretical security breach scenarios. In a controlled lab environment, students acquire hands-on experience by directly examining several common vulnerabilities and countermeasures, including cross site scripting, sql injection, and Android malware and rootkits. They also perform pen testing experiments using Kali Linux and compete in a "capture the flag" pen testing competition. We have partnered with the Networking and IT department at Fairmont State, allowing students to gain professional skills by deploying two common vulnerability scanner software systems, NMAP and Nessus Home, and creating vulnerability assessment reports of various networks on campus that they present, as a group, to campus networking professionals. In the future, we are adding training with the popular SIEM software QRadar through a series of exercises implementing and operating a small scale SOC in the cybersecurity lab on campus

National Securities and Intelligence (NSI) Program

The biggest demand at the federal level is in the Departments of State, Defense, Justice, and Homeland Security, as well as the traditional opportunities at the Central Intelligence and National Security Agencies. The NSI program is designed to provide students with the tools they need to pursue those career goals as research and/or intelligence analysts.

The Open Source Intelligence Exchange (OSIX) is the laboratory and applied research component of the University's NSI program. Student analysts work with faculty mentors to engage in intelligence gathering from open sources. OSIX students receive state of the art practical experience and share their work with real customers in the national security and law enforcement communities. The CIA, FBI, Department of Defense, and Department of State, as well as to state and local law enforcement agencies in West Virginia have received intelligence products from Open Source Intelligence Exchange students.

Information Systems Management (ISM) Program

Fairmont State University offers a Bachelor's of Science (BS) degree in Information Systems Management (ISM) that encompasses operating systems and network technologies, software application development, web technologies for mobile and cloud platforms, software application testing and secure coding, big data and data analytics, machine learning principles and tools, information assurance and cyber security, and project management principles and practices.

Along with a breadth of topics the students complement their knowledge by gaining real world experiences on projects related to Enterprise Networks and Solutions, Project Management, Software Application Development and Testing, and Information Assurance and Cyber Security. Some example projects include working with local police

department's students provided threat analysis and vulnerability assessments on local law enforcement IT infrastructure. Students developed image processing software used for identifying threats in seized digital assets. Students developed machine learning applications that utilized open source social media data for threat intelligence. Students also provided threat and risk assessments for local businesses near campus.

Automation and Robotics

Fairmont State University offers a minor in Automation and Robotics which provides a multidisciplinary approach for the skills and knowledge needed to design, implement, and troubleshoot embedded, automation, and robotic systems that are being realized across multiple industries such as manufacturing facilities, healthcare industry, automotive industry, power generation plants, etc.. With an increase in these technologies it is important for students within the Mechanical and Electrical Engineering or Computer Science programs to be able to complement their discipline knowledge with a minor in automation and robotics.

Fairmont State hosts several state, regional, and national robotics competitions throughout the year providing all of its students with hands on practical experiences. These robotic initiatives have grown considerably across the state increasing the interest of future students but in industry realizing there is a workforce in WV that can be relied upon.

Resource Needs:

The state-of-the-practice experiential learning obtained at Fairmont State University in Computer Science, Cybersecurity, National Security and Intelligence, and Information Systems Management prepares students to be leading members of the cybersecurity workforce in West Virginia and the nation.

Our forward-thinking field experts and scholars have positioned Fairmont State University to be a leading authority in educating the future workforce of West Virginia (WV). The experiential learning conducted in the classrooms is a result of the collaborations established with industry and government. These collaborations help ensure the curricula are at the cusp of innovation, relevant and valuable to government, industry and to students.

To continue this exceptional service and push to greater heights, Fairmont State University seeks to become a NSA National Center of Academic Excellence in Cyber Operations and a DIA Intelligent Community Center of Academic Excellence.

Financial resources in the amount of $1.6 million are sought to achieve the vision outlined above, and the specifics outlined below. This funding will enable Fairmont State University to position West Virginia and the University as the hub for Cybersecurity in the nation.

Tools and computing resources:

- Security Operations Center (SOC) – establishing a SOC on the University campus to secure the University's digital assets as well as local towns and state governments that wish to utilize the resource. This Operations center would enable advanced research to be conducted to grow the University's research capabilities as well as provide experiential learning to its students.
- Cyber range in the cloud – establishing hands-on cybersecurity learning is paramount to fulfilling the needs of industry and government. To date, Fairmont State University has done a tremendous job in providing hands-on learning in the classrooms. With the University's aging laboratories, funding is needed to enhance its classroom laboratories as well as support advanced research conducted by the faculty.
- Open Source Intelligence Exchange (OSIX) – the OSIX laboratory and applied research component of the National Security and Intelligence (NSI) program provides exceptional learning opportunities for the University's students to put into practice what is taught in the classroom. The OSIX laboratory is also a major service provider to the Intelligent Community within the state of WV. Additional resources are needed to enhance the laboratory's computing platforms as well as well as enhance the software tools utilized.

- Community Outreach – Additional funding will support the online delivery of courses across the state to all of WV's high schools to better prepare the high schools students to enter the cybersecurity disciplines. Advanced cyber labs will be established with all the high schools across the state, connected to Fairmont State's cyber-labs so that training and skill development can be provided remotely across the state by University professors.

- Professors, Certifications, and Curriculum Development:
  - All cybersecurity-related classes offered at the University provide real world, hands-on semester projects in order to enhance the student's practical skills as well as allow the University to be a leading service provider in the state. Additional internships and collaborations are required for these kinds of value-added projects and must be integrated across the state.
  - Additional professors are needed to support the growing demand of cybersecurity students. Three professors will be added to the cybersecurity disciplines in order to support the growing need of classes as well as to conduct cutting-edge research to address cybersecurity challenges.
  - Masters of Business Administration (MBA) concentration in cybersecurity will be established in the Fall of 2019 to enhance the knowledge, skills, and abilities of the professionals working in the state of WV.
  - The University will establish collaborations with appropriate organizations. Certifications in cybersecurity will be offered to Fairmont State University's students and to the public at-large. The University will offer training and testing facilities/materials such that its trainees can affordably acquire the certifications required by the government and industry.
  - The University will establish a conduit for Veterans, active duty reservists, and Guard men and women to utilize their unique skills and abilities. This initiative will advance offerings of the University by providing advanced strategies (computing platforms, remote offerings, etc.). It will also make the training and University degrees more accessible via online classes to better serve the needs of this population throughout the state and the nation.
  - The University will establish a mentoring program and advanced training facility for the workforce of WV to be retrained in the cybersecurity-disciplines. The workforce in WV needs to have an avenue to retool and be retrained in new skills. The University's coaching and mentoring program will help retrain members of the nation's armed services coming off active duty, employees that have been displaced, and employees that desire a career change.

  - Fairmont State University is a force multiplier in addressing the workforce challenges facing the state.

Marshall University

Marshall University provides cybersecurity offerings at both the College of Information Technology and Engineering (CITE) and within the Digital Forensics and Information Assurance (DFIA) program.

Marshall University College of Information Technology and Engineering (CITE)

1. An overview of cybersecurity offerings and specialties

The College of Information Technology and Engineering (CITE) has an aggressive plan to produce hundreds of undergraduate and graduate students every year in Computer Science, Information Systems, Computer and Information Security, and Cybersecurity. The Weisberg Division of Computer Science in CITE at Marshall University offers a new Bachelor of Science (BS) degree program in Computer and Information Security beginning in fall 2018. CITE has also offered an online Graduate Certificate in Information Security with 15 hours of course credit for many years for students pursuing security positions in the federal and private sectors.

The MS in Information Systems and the MS in Technology Management in CITE incorporate elements of Cybersecurity in the curriculum that will allow key personnel in the managerial capacity to properly design, manage and strengthen the security of their cyber infrastructure. The current offering of BS and MS in Computer Science provide critical elements needed for Cybersecurity professionals such as networking, data

analysis and programming. CITE is discussing the potential with many industries and partners to create pathways for students' success with internships and co-op programs. The College is also working on the development of 2+2 with community and technical colleges.

Collaborative and cutting-edge research in cybersecurity is expected to be conducted in partnership with other universities and research institutions along with industries and government entities at the state and federal level. Current faculty research in the Weisberg Division of Computer Science includes cryptography, IoT security, mobile and wireless network security, penetration testing and prevention, and more.

The Division is specifically committed to ensuring that the graduates from the program will strengthen the Cybersecurity workforce and fill in the current needs. The degree programs offered and its graduates will contribute to West Virginia's economic development and advance its competitive edge regionally, nationally and globally.

2. **Information about how the institution is ensuring that cyber graduates have "hands-on experience with the latest tools and techniques ready to hit the ground running."**

The Weisberg Division of Computer Science aims to strengthen the quality of the program through several focuses:

- *Strength of Knowledge Body:*
  The BS in Computer Science program in the Weisberg Division of Computer Science at Marshall University recently received accreditation from the Accreditation Board for Engineering and Technology (ABET) and we expect the new BS in Computer Science and Information Security program will be among the first programs in the nation to earn ABET accreditation as well. The curriculum for the Bachelor of Science in Computer and Information Security is designed to meet the requirements of ABET's Computing Accreditation Commission for Cybersecurity. This ensures that the course offerings and the topics covered are in accordance to the current and future needs of Cybersecurity professionals. In addition, the curriculum is also aligned with Knowledge Unit (KU) requirements of the National Center for Academic Excellence in Cyber Defense (CAE-CD) sponsored by the Department of Homeland Security (DHS) and the National Security Agency (NSA). The CAE-CD Knowledge Unit requirement will ensure each graduate to have critical core technical and non-technical knowledge along with an optional knowledge unit that covers specific topics in the field of Cybersecurity. By aligning the curriculum with two national standards, graduates of the program will have the necessary and most up-to-date skills and knowledge that are currently needed in the field of Cybersecurity. In addition, the curriculum will also prepare students to obtain Cybersecurity certifications that are currently used in the industry such as the Certified Ethical Hacker (CEH), Palo Alto Networks Certified Network Security Engineer (PCNSE), Certified Information Systems Security Professional (CISSP), Cisco Certified Network Associate Security (CCNA-Security) and CompTIA Security+.
- *Strength of Research:*
  Faculty of the Weisberg Division of Computer Science are constantly engaged in scholarly activities related to Cybersecurity. The research encompasses the fields of Wireless Security, Data Analytics, Machine Learning and Internet of Things Security that will enrich the academic side of the program along with opening opportunities for students to be the producer of future technologies.
- *Strength of Experience:*
  Students in the Computer and Information Security program will be involved with Cybersecurity projects through internships and research projects. The curriculum requires students to complete at least one semester of internship prior to graduation. In addition, students will also participate in competitive events and activities such as the National Collegiate Cyber Defense Competition and DEFCON contest among others. Students will also be expected to increase interest in the field of

Cybersecurity by providing mentoring to youth groups through activities such as the Cyber Patriot Camp and the Cyber Patriot Competition. The Division successfully hosted the first and only Cyber Patriot Camp in West Virginia in July 2018 and will continue to offer the camp along with the advanced Cyber Patriot Camp in the following years.

- *Strength of Collaboration:*
  The Weisberg Division of Computer Science has existing collaboration with federal and state entities along with industry collaboration that will allow internship opportunities and placement of graduates in the cybersecurity field immediately after graduation. The strength of collaboration will also open the opportunity to imbue the course offerings to include the latest and cutting edge topics in the field of Cybersecurity. The Division is also planning to partner with other higher education institutions in the area to create a 2+2 agreement, faculty exchange and other collaborations that will ensure that graduates of the program will be able to meet and exceed the current requirement for a cybersecurity professional.
- *Strength of Infrastructure:*
  The Division houses several labs including a networking and cybersecurity lab that incorporates an internal network within the lab which allows for full environment simulation that reproduces a target environment, as closely as possible, rather than relying on virtual machines and virtual networks. For example, the lab will allow students to practice penetration testing through the simulation of a corporate environment within the lab without affecting the existing university network. This lab is housed in the Arthur Weisberg Family Applied Engineering Complex and is the only one of its kind at Marshall University.

3. **Details on what additional resources, if any, will be needed by your institution to provide <u>more or expanded</u> learning opportunities to meet the growing employment opportunities in the cybersecurity world.**

The Weisberg Division of Computer Science in CITE at Marshall University offers the B.S. in Computer and Information Security and the M.S. in Cybersecurity program (waiting for BOG approval). The curricular of the programs were designed to satisfy the ABET Cybersecurity accreditation and cover core Knowledge Unit (KU) of National Centers of Academic Excellence in Cyber Defense (CAE-CD). Faculty members in the Weisberg Division of Computer Science have demonstrated expertise in the area of cybersecurity with strong research and publication records. Their specific interests include security in computers and networks, mobile and wireless networking, Internet of Things (IoT), cloud computing, and quantum computing, etc. The division is very active in K-12 education in Cybersecurity working with local middle/high schools and hosted the first and only Cyber Patriot Camp in West Virginia in summer and plan to provide training/retraining of cybersecurity workforce in WV at entry-level cybersecurity jobs. Since employers frequently look to certification as an important measure of excellence and commitment to quality, we examine possible cybersecurity certificate programs in the division preparing students for cybersecurity job market without going through regular degree programs such as CompTIA Security+, GIAC Security Essentials at the entry level as well as more advanced level certification such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Information Security Manager (CISM). The division runs multiple state-of-the-art computer labs for teaching and research including dedicated Cybersecurity lab. Based on division's interest and plan for providing advanced and expanded learning opportunities to students and building workforce in cybersecurity fields, following additional resources will be very beneficial:

1. Building Academic Partnership to provide cybersecurity certifications

Establishing partnership(s) with certification entities in cybersecurity will cost extra fee and expense to the division but students will have better access to the learning and testing materials and reduce the certification exam fee.

2. *Equipment and maintenance of facility*:

To properly utilize the existing infrastructure built into the networking and cybersecurity lab and other computer labs at the College of Information Technology and Engineering, the labs will need to be supplemented with various software and hardware that can emulate various cyber infrastructures that are currently used in the field. Networking hardware along with sandbox server will allow students to have hands-on experience with actual cyber infrastructure. To emulate a Secure Operations Center (SOC), labs with display wall that can provide situational awareness of the current state of the infrastructure. In addition, to ensure that such software and hardware are properly deployed and maintained and student assistants will need to oversee the day-to-day operation of the lab both for academic and scholarly activities. Lab assistants will assist the lab administrator hired by Marshall University to develop and deploy the lab for classroom and research activities.

Based on our Strategic Plan submitted above in Aug. 2018, we request following *estimated* budget* to support it:

Item	Description	Qty	Amount
Networking Equipment	Networking equipment for SOC	5	$50,000
Servers	SOC Sandbox Servers to run virtual machines	3	$12,000
Displays	SOC Scoreboard display	2	$10,000
Student Assistants	Four student assistants working 20 hours/week for $12/hour per year (50 weeks)	4	$48,000
Academic Partnership	Academic Partnership Membership and Service Fee	5	$10,000
Certificate Exam Fee	Vouchers for students to take certifications exams	100	$10,000
Total			**$140,000**

** -The budget above is to support and cover the initial costs for one year without any indirect cost involved. For a 5-year plan, financial resources in the amount of $700,000 will be needed to achieve the vision outlined above --supporting more labs and increased number of students in the programs.*

Marshall University Digital Forensics & Information Assurance

The Marshall University Digital Forensics and Information Assurance program produces graduates that can use science and technology to solve investigative and cyber security problems. The program is practitioner focused, intent on providing students with the education and skills they need to help fill the cyber security skills gap. The DFIA program emphasizes critical thinking, problem solving, and communication. The curriculum is delivered in a challenging, hands-on environment, using many of the same professional tools, techniques, and procedures they will use upon entering the workforce. The MU DFIA program is also seeking the NSA and DHS designation for National Centers of Academic Excellence.

Undergraduate Curriculum

Courses taught in the curriculum reflect our focus on the practitioner and the skills and education they need. The curriculum includes cyber security classes that develop both offensive and defensive skills. Some of our courses include Network Penetration and Attack, Network Defense, Cyber Warfare, Web Application Penetration Testing, Applied Digital Forensics, Network Forensics, and Mobile Forensics among others.

All of our core courses contain separate lab sections where students hone their digital forensics and cyber security knowledge and skills. Students get extensive experience using industry standard tools such as AccessData's Forensic Toolkit, Kali Linux, Cellebrite, WireShark, Social Engineering Toolkit (SET), Network Miner, Metasploit, Armitage, NMAP and many others. Students are able to take certification tests for both AccessData and Cellebrite forensic tools.

MU DFIA Lab exercises focus on building discrete skills that culminate in realistic projects or scenario-driven problems requiring students to apply what they learned during the semester.

These culminating exercises are developed with realism in mind. Take DFIA 460 Applied Digital Forensics for example. At the end of the class, students are given are given digital evidence from a simulated arson case. The students perform the examination and analysis and deliver a realistic final report. Many of our courses include this type of problem-based learning assignment.

The program concludes with an intense capstone experience where students put their knowledge and skills to the test by working through challenging simulated cases, penetration tests, and real-world cyber security problems. This capstone experience is designed to assess and reinforce the major learning objectives from all of the program's core courses.

Learning Outside the Classroom

The opportunities to learn don't stop when the students leave the classroom. Students are afforded additional skill-building opportunities through internships, research projects, the Colligate Cyber Defense Competition (CCDC) team, and our Open Source Intelligence Exchange (OSIX). The OSIX uses selected, vetted students to do real-world open source intelligence collection and analysis. We do this work for various clients including law enforcement, NASA, the WV Intelligence Fusion Center, and Operation Underground Railroad (OUR). The MU OSIX works closely with Operation Underground Railroad to help fight international child sex trafficking. MU DFIA students have provided intelligence that has assisted in the rescue of 40 children and the arrest of 10 suspected traffickers.

Students also engage in applied research guided by faculty. Some of the research topics include vehicle forensics, voting machines, wearable devices with geolocation, FitBit, etc.

Students can also gain practical skills through several conferences including Blackhat, DerbyCon, AIDE, and SecureWV. Students can attend AIDE and SecureWV free of charge and compete against professionals in capture the flag and network king of the hill events. Our students also have access to the BlackHat Student Internship Program that allows students a paid week helping to organize the BlackHat cyber security conference in Las Vegas. Students are given room and board as well as exclusive access to conference to workshops, lectures, and exclusive VIP networking opportunities.

Looking Ahead

We will be launching a graduate program in Fall 2019. Like our undergraduate program, our MS degree will also be practitioner-focused. We are also working on additional ways to prepare our students to pass the industry standard certifications most often sought by employers. "Bootcamp" style preparation courses are also being planned for the summer of 2019.

As far as additional resources, funding would be at the top of list. We could use money to offset the costs related to development and creation of practical lab exercises, case simulations, table top exercises, and the like. Undergraduate and graduate students, working at the direction of faculty, could provide very cost-effective labor for this effort. Additional funds could also be used to offset the costs for more applied research (i.e. costs of consumer products, software, tools, etc.). Lastly, funding could also be used for student and faculty activities outside the university (conferences, etc.). Another potential need would be administrative assistance to help manage the NSA/DHS CAE program paperwork.

Marshall University Master's Degree Program in Forensic Science

The Master's degree program in Forensic Science offers an area of emphasis in digital forensics. The course offerings within the digital forensics curriculum merges classroom instruction with practical, laboratory-based training. The latter culminates with students taking the Access Data Exam (ACE), successful completion resulting in a certificate.

Those students pursing the digital forensics area of emphasis also benefit from having a working digital forensics unit housed within the MU Forensic Science Center. Although our students cannot be directly involved in criminal casework, mock exercises have been developed that simulate actual cases and allow students to use the Cellebrite mobile forensic tool, AccessData FTK 6 and other forensic software. Students have performed research projects on drones, automobiles, Alexa and copy machines to determine the type and amounts of stored data that could serve as evidence in criminal investigations.

Resource Needs:

As far as additional resources are concerned, funding would be at the top of list. Funding would be used for:

- Additional lab, teaching space and equipment.
- Development and creation of more practical, hand-on lab exercises, case simulations, table top exercises, and the like.
- More applied research (i.e. costs of consumer products, software, tools, etc.).
- Student and faculty activities outside the university (conferences, etc.).
- Administrative assistance to help manage the NSA/DHS CAE program paperwork.

Together, this amounts to $140,000:

- Lab Equip & Furnishings - $75,000
- Academic Lab Exercise Development - $10,000
- Test devices for Applied Research - $10,000
- Student & Faculty External Activities - $15,000
- Faculty Training - $15,000
- Admin Support for NSA - $15,000

University of Charleston

The University of Charleston West Virginia (UCWV) offers two cyber security degrees inclusive of a 2 Year Bachelor of Science in Cyber Security (BSCS) degree completion program emphasizing certifications as a part of the curriculum (e.g. Certified Ethical Hacker, Certified Incident Handler, and Certified Security Analyst). The University will pursue a four year in-seat Bachelors degree to further provide hands on teaching and technical skills for the traditional student exiting high school, amongst other sources. The Masters of Science in Cyber Security (MSCS) emphasizes program management curriculum that has been mapped to the NIST framework, to learn the leadership skills necessary in today's Cyber Operations and Defensive based organizations.

Bachelor's of Science in Cyber Security:

The Bachelor's degree consists of approximately 50% of the curriculum inclusive of hands on techniques, ethical practices, and ilab environment activities in partnership with ECCouncil where UCWV is an Accredited Training Center.

Hands on Activities include, but are not limited to:

- Ethical Hacking,
- Incident Handling,
- Security Auditing,
- Initial Forensics,
- Enumeration,
- Network Analysis, and
- Security Trending Analysis.

The mission of the Bachelor of Science in Cyber Security (BSCS) is to provide graduates within the program with the ability to apply learned skills and experiential knowledge of security technology to make a significant contribution to the information security of individuals, corporations, governmental services and the national community. The following represent the program outcomes for the BSCS:

Outcome 1: The graduate will establish and supervise legal and ethical practices in the cyber security arena.
Outcome 2: The graduate will develop and implement a comprehensive cyber security strategic plan for individuals, corporations, governmental services and/or the national community.
Outcome 3: The graduate will detect, assess, and remediate ongoing cyber security threats and vulnerabilities.
Outcome 4: The graduate will effectively communicate cyber threats and remediation strategies across organizational levels in both verbal and written formats.
Outcome 5: The graduate will integrate technical knowledge, software and hardware capabilities, and threat and vulnerability awareness across varying technology formats such as operating systems, networking, social media, mobile, and handheld devices.

Masters of Science in Cyber Security:

The Master's degree picks up where the Bachelor's degree leaves off where students in the Bachelor's degree can matriculate into the Masters to learn the managerial and leadership skills necessary in today's Cyber Operations and Defensive based organizations.

Hands on Activities include, but are not limited to:

- Financial ROI/NPV Analysis,
- Intelligence Collection and Analysis,
- Data Analytics,
- Cyber Operation Analysis,
- Information Assurance Tactics,
- Synthesis of Legal Cases,
- Research Based on Cyber Trends and Forecasts.

The mission of the Masters of Science in Cyber Security (MSCS) is to educate graduates to make a significant contribution, with a commitment toward moral purpose and productive work, within the information security community in support of individual, corporation, governmental services and organizational strategic goals. The following represent the program outcomes for the MSCS:

Outcome 1: The graduate will evaluate and defend the mission of an organization requiring security defense by analyzing the needs and costs of creating security related programs and strategies.
Outcome 2: The graduate will analyze the demands of systems security and practiced methodologies for protecting data integrity and confidentiality through ethical practices.
Outcome 3: The graduate will synthesize a variety of challenging policy, legal, and technological concepts in relation to cyber security.
Outcome 4: The graduate will evaluate security theories, apply experiential lessons learned, evaluate new research and generate new research and security models for organization's who require security related and information management strategies.

Workforce and Economic Development Recommendations:

We recommend that a proactive strategy be developed to make West Virginia the nation's leading destination for cyber and information security education. Doing so will require identifying key career pathways, the research and programs needed to prepare people for each pathway, and a collaborative approach to program development across institutions that maximizes pathway impact and minimizes within-state competition.

A recent article on cybersecurity degree differentiation across colleges and universities in Indiana illustrates such possibilities. While the distinct character of the IU, Purdue and other programs may not have been intentional from an indirect competition standpoint, being strategic in how our WV universities distinguish their cyber programs is a smart model. Being proactive in this regard will pre-empt direct competition between institutions, when we should be competing against other states for students and future workers. Collaborating should also generate positive external equity and open up public-private funding opportunities for all. If done effectively, we can present WV as the nation's leader in cyber security education through offering a rich portfolio of distinct programs across our institutions.

UC welcomes the opportunity to participate in and lead this effort.

Other specific recommendations include:

- Training opportunities in technological initiatives to include building knowledge in programming, analytics, security, intel, operations, defensive tactics, and ethical practices. UC is developing new degree programming in data sciences, coding and computer programing that can be integratedinto future cyber programs.
- A shared or collocated cloud-based lab environment would be of assistance to many Statewide resources who can pursue the technical skills necessary through online training programs to include certificates, MOOCs, specific training needs, and/or skill-based offerings as deemed by organizational needs.
- Internship opportunities would also be of added value to funnel individuals through the aforementioned training, while helping to ensure the resources stay within the organization, and within the State of WV.
- Shared research opportunities that can provide the State, organizations, and academic institutions with a shared responsibility to grow cyber knowledge, collectively.

West Virginia University

1) **Provide an overview of your institution's cybersecurity offerings, specialties and degrees.**

Starting Fall 2018, WVU has expanded its cybersecurity offerings with new degrees and certificates in Computer Science and Business Cybersecurity Management.

Computer Science Offerings:

The new undergraduate degree in Cybersecurity is offered by the Lane Department of Computer Science and Electrical Engineering and provides students with a solid foundation in programming, Computer Science, and core technical aspects of Cybersecurity through courses such as Foundations of Cybersecurity, Cybersecurity Principles and Practice, Secure Software Development, Host Based Cyber Defense, Practicing Cybersecurity: Attacks and Countermeasures, and Computer Incidence Response. In addition, the program includes interdisciplinary courses in Cryptography, Information Ethics, and Cybercrime to allow a well-rounded perspective on the field. Students will have the chance to choose between electives exploring software design, artificial intelligence, computer forensics, networking and databases.

To supplement the new degree, undergraduate students who are already majoring in Computer Science, Computer Engineering, and Biometrics Systems can add an Area of Emphasis in Cybersecurity which consists of a sequence of five courses; while undergraduate students of other majors can receive a Minor in Cybersecurity by completing a sequence of six courses.

In addition, WVU is in the process of reorganizing the existing Graduate Certificate in Computer Forensics as a Graduate Area of Emphasis in Cybersecurity. WVU is designated by NSA/DHS as a National Center of Academic Excellence in Cyber Defense Education and in Cyber Defense Research. The new educational initiatives leverage

existing strengths and aim to produce work-force ready cybersecurity experts and increase the prospects of enhanced economic development for West Virginia.

Business Cybersecurity Management:
The College of Business and Economics now offers a Master of Science in Business Cybersecurity Management (CYBR) and Minor in Business Cybersecurity Management, both situated at the intersection of business and cybersecurity management. The program focuses on developing the managerial and technical skills needed to identify weaknesses, manage vulnerabilities, protect assets, defend networks, and audit the security of information systems. Learning is accomplished in an online environment using hands-on vulnerability assessments, statistical analyses, and risk-based decision making. Business Cybersecurity entails optimizing the management of protection of a company's hardware, software and information assets as well as preventing the disruption or misdirection of those assets. Part of the CYBR initiative in the WVU College of Business & Economics is to help our partner organizations better understand and develop their cybersecurity effectiveness. This allows organizations to partner not only with students, but also with faculty on advanced cybersecurity projects that can result in co-branded publications. West Virginia University is working with IBM and other organizations to provide general IT, software development and cyber security training to increase the number of qualified candidates for in state companies. The first class began in August, 2018, and, with little advertising, has already enrolled 14 graduate students.

2) **Provide information about how the institution is ensuring that cyber graduates have "hands-on experience with the latest tools and techniques ready to hit the ground running." This should include addressing this statement by Greg Blaney:**

> "NASA IV&V along with the rest of the Federal Agencies are in desperate need of folks possessing both integrity and cyber security skills. And I'm not just talking about academic training; we need folks with hands-on experience with the latest tools and techniques ready to hit the ground running. Here at NASA IV&V, we are setting up a training lab which will allow folks to train in ethical cybersecurity activities as well as participate in cybersecurity competitions. I suggest the more we partner in providing hands-on activities here in the state, the more WV will be able to lead in the cybersecurity area."

The WVU Computer Science Cybersecurity programs include classes with hands-on activities using available tools, programming assignments, and term projects. Moreover, the BS in cybersecurity has two capstone courses for which students will work in groups to design and implement cybersecurity related projects. The Statler College, home of the Lane Department of Computer Science, has excellent working relationships with a number of area businesses including Leidos, KeyLogic, NASA Independent Verification and Validation Facility and the FBI's Criminal Justice Information Services Division; all of these are excellent future partners for internships and training opportunities for students in the Cybersecurity program. Additionally, many governmental employers require applicants to have a degree from a designated Center of Excellence in Cyber Defense, a designation which WVU already has. The formal course offerings are supplemented by less formal cybersecurity related student organizations. In particular, CyberWVU is open to all undergraduate and graduate students. Students and faculty meet regularly, work on different hands-on cybersecurity topics, and compete in multiple competitions throughout the year.

The WVU Business Cybersecurity Management program is suitable for participants from a broad range of backgrounds who have interest in a career in cybersecurity. The program is a combination of online coursework, which allows students the flexibility of maintaining a career, that is augmented by two, two- to three-day residencies where they focus on experiential learning. Coursework includes Business Intelligence, Data Management, Information Security Assurance Management, Data Communications, Network Security, Cybercrime Management, Ethics and Legal Procedures, Fraud Data Analysis, Business Data Visualization and a capstone business cybersecurity practicum class. Learning is heightened through obtaining certifications, working in teams, professional communication, lab based problem solving and engagement with real-world business cyber

challenges. Project work includes working with a client organization to provide an analysis, data collection and a recommended solution to cybersecurity business problems. Students may also obtain temporary placement with public or private enterprises for professional competence development.

3) **Providing details on what additional resources, if any, will be needed by your institution to provide <u>more or expanded</u> learning opportunities to meet the growing employment opportunities in the cybersecurity world. These details will be provided to Matt Turner at the HEPC and the aggregated as part of the final report.**

The high-quality instruction we envision for experiential and hands-on cybersecurity learning, combined with training in research/thought leadership and continuing/executive education, demand an investment in personnel and infrastructure in order to grow and nurture a robust pipeline of cybersecurity talent in WV. Already, both new WVU cybersecurity programs have experienced significant interest even in their first year. Over 100 students are currently enrolled in the CS and Business cyber courses with no advertising of the new majors as of yet. These programs will clearly require additional resources to fully address the pent up demand. The addition of three new faculty lines in each program (total 6 new lines) would significantly accelerate the program development, allowing WVU to leverage existing cybersecurity expertise and our growing industrial and federal partnerships, and to utilize NSA Center of Excellence designations in order to become a regional powerhouse for interdisciplinary cybersecurity education and research. Furthermore, there is significant ancillary benefit to WV by aligning the research efforts of these new hires with regional business priorities. This provides routes to externally funded projects supported by SBIR/STTRs with concomitant economic development opportunities. These new investments in essential faculty require salary and benefits support at the level of $750K/yr.

In addition to personnel, state-of-the-art programs call for on-campus cybersecurity labs that provide "sandbox" infrastructure to permit simulated cyberattacks, that are as realistic as possible, but that do not compromise functioning university systems. These facilities allow for the hands-on learning that employers expect. Such laboratories consist of a network of devices, including a variety of PCs, as well as mobile devices and industrial controllers, which reflect the assortment of information infrastructure that is subject to cyber attacks. The devices are networked behind a hardware router and firewall to separate them from the university computing network, and allow flexible experimentation for both teaching and research. The sandbox should also include the capability to simulate a larger virtual network of machines in a cloud-environment such as Amazon Web Service, to prepare students for realistic network scenarios. The infrastructure would require a one-time capital investment of $300K and need the supervision of a paid full-time Teaching Associate with IT experience at the rate of $75K/year including benefits.

These investments at a critical juncture in the development of the WVU Cybersecurity programs will fast track the programs to provide maximum benefit and opportunity to both WV students and the our growing cybersecurity economy.

In addition, two state higher education institutions are developing new cyber learning opportunities:

<u>Bethany College</u>

Bethany is planning to provide two majors in Cybersecurity: one leading to the Bachelor of Arts degree and the other to the Bachelor of Science degree. The Bachelor of Arts plan is designed for those students seeking a career in information assurance that focus on the identification of threats and vulnerabilities in order to protect business and government digital systems. Students in this major complete courses in programming, project management, computer security, ethics, computer organization and assembly language, network architecture, computer forensics, operating systems, network security, operating system security, principles of management, writing in the field, senior project, and a comprehensive exam at the completion of the program. The Bachelor of Science plan is designed for students seeking a career in cybersecurity focused on the research and development of software and systems for protecting digital assets. Student in this major complete courses in programming, computer security, data structures, computer forensics, two courses in calculus, calculus-based probability and statistics, cryptography,

numerical analysis, network architecture, network security, operating systems and security, writing in the field, senior project, and a comprehensive exam at the completion of the program.

Bethany plans to ensure the provisioning of hands-on experiences with the latest tools and technology:

ZeroChaos Cybersecurity Lab

Through a donation from ZeroChaos, work force management company, and efforts of a Board of Trustee Doug Goin, the ZeroChaos Cybersecurity air-gap lab has been established on-campus. The lab space is dedicated to the student learning experience in a variety of courses. This set of computers that will operate on a completely separate network to allow students the opportunity to learn in a protected environment.

IBM Mainframe z System Certification

There is high demand in the private sector currently for those individuals who can program mainframes. Bethany College, through an alumni connection, is offering the interested student the opportunity to gain professional certification for his/her skills in working with IBM mainframes. Through the IBM mainframe z System, a foundational knowledge of the COBOL programming language and the IBM "Master the Mainframe" z OS training is being offered for the students. The students are taught an introductory component in the Computer Science I course and then offered a series of trainings to assist them in earning professional certification.

Advisory Board

Alumni, trustees, and members of the community will be serving on an advisory board for the major. The board will advise the program on the skills and technology that the field is looking for from students. This will provide the faculty quick feedback on ways to improve the program and to keep Bethany students current in the field.

Bluefield State College

Bluefield State is in the process of creating a minor in cybersecurity within computer science (with full implementation in 2019), offering the following courses:

- COSC 241 Intro to Linux/Unix (3 CH)
- COSC 342 Computer Forensics (3 CH)
- COSC 382 Penetration Testing (3 CH)
- COSC 404 Ethical Hacking (3 CH)

This minor will be available in 2019.

8. CyberSecurity Offerings – W.Va. Two-Year Institutions

Provided is information on cybersecurity programs and degrees offered by the state's community & technical college system.

Blue Ridge CTC

The Cyber Security program at Blue Ridge offers an Associate of Applied Science Degree, incorporating vendor certification training, for students preparing for entry-level employment or advancement in a variety of occupations and courses in Cyber Security. The program offers students the opportunity to select one of two tracks; Network Security Hardware or Network Security Application. These two tracks will provide the student with the knowledge to enter the Cyber Security workforce and/or transfer to a four-year institution for further undergraduate education. Students will complete hands-on activities that will provide an overview of basic principles and security concepts related to active mitigation of known common threats. The curriculum discusses risk, threat, and security assessments and utilizing them to develop security policy, business continuity, disaster recovery, and incident response planning. The program also covers security methods, controls and procedures, ethics, laws, and computer forensics. In addition, the program describes the use of cryptography as a tool, software development processes, and protection. Students will develop an understanding of the information assurance progression and how they can apply this knowledge to support their organization. Industry certifications within cyber security include:

- Certiport IC3
- CompTIA A+ (Jumpstart)
- CompTIA Network+
- CompTIA Security+
- Linux LPI I and LPI II --- combined makes CompTIA Linux+
- Cisco Certified Entry Level Network Technician (CCENT)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Associate – Security (CCNA-Security)
- Cisco Certified Network Associate – Wireless (CCNA-Wireless)
- Cisco Certified Network Professional – (CCNP)

BridgeValley CTC

The Cyber Security A.A.S degree program at BridgeValley provides a general background in computer repair; computer networking; internetworking; enterprise computing practices; implementing and maintaining security on computers and networking equipment; and assessing security risks. The breadth of coverage produces a multi-skilled entry-level information technology "jack of all trades" with a high degree of career flexibility in large business organizations and the ability to independently handle the information technology needs of small and medium size businesses. Industry certifications within cyber security include:

- Cisco Certified Entry Networking Technician (CCENT)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Network Associate Cyber Operations (CCNA Cyber Ops)
- Routing Pro
- Switching Pro
- Security Pro, also eligible to take the ComPTIA Security +

Mountwest CTC

The Associate in Applied Science Degree Program in Network Systems Security offers comprehensive network training from Mountwest Community and Technical College's Microsoft Information Technology Academy and Cisco Networking Academy. Within the two-year Associate Degree program, students take courses developed by Microsoft and Cisco, providing specialized skills in network administration, design, and security. Industry certifications within cyber security include:

- CompTIA's A+ Hardware and Operating Systems
- Microsoft's MCSA: (Microsoft Certified Solutions Associate)
- CompTIA's Linux+
- Cisco's CCNA (Cisco Certified Network Associate)
- CompTIA's Security+
- CompTIA's Server

The program is designed so graduates will be capable of performing network administration, design, maintenance, and security on a variety of network operating systems and devices.

- Microsoft Certified Solutions Associate manage and troubleshoot system environments running the Windows 2008 operating system.
- Cisco Certified Network Associates design, build, and maintain computer networks using a variety of network devices.
- CompTIA Security+ and Cisco Network Security Specialists design and implement security solutions that reduce network vulnerability.
- Cisco Wireless LAN Support Specialists implement and troubleshoot Wireless LANs.

MCTC's Network Systems Security option provides fundamental networking knowledge and skills with specific network security training crucial for entry into information security positions in public corporations and government entities.

Pierpont CTC

The Associate of Applied Science degree in Information Systems Technology with a concentration in Cyber Security provides students with valuable skills and knowledge in computer and network design, installation, support and computer and network security. The program enables and encourages students to learn essential problem-solving skills, industry best-practices, software applications, and core technical skills used by information systems and technology industry professionals. Additional Cyber Security skills will focus on intrusion prevention and detection, proactive support and penetration testing. Industry certifications within cyber security include:

- Cisco CCENT (only AAS)
- CompTIA A+ (only AAS)
- CompTIA Security + (AAS and CAS)
- EC Council CEH
- EC Council CND

WV Northern CTC

The Associate in Applied Science degree in Computer Information Technology with a concentration in Cyber Security is prepares students to:

- Identify the scope of security problems, identify risk assessment, and describe malicious logic and security policies
- Identify major concepts of theories used in Cloud computing and architecture
- Describe Cloud ROI models, deployment models, and Cloud computing implementation
- Identify hacker attack techniques and methodologies, network worms, viruses, and malicious code, computer crimes, organizational intelligence regarding their technologies, and information technology warfare
- Identify major concepts used in cyber security, and psychological influences of cyber security
- Describe the mentality of a hacker and a hacker's manifesto
- Identify major concepts regarding network security and abnormal networking behavior and its causes
- Describe network defense fundamentals, concepts related to managing firewalls, and the use of Intrusion Detection Systems.

Industry certifications within cyber security include:

- EC- Council CEH
- CompTIA Net +
- CompTIA A +
- Cisco CCNA
- Cisco CCENT
- CompTIA Sec+

WV Northern CTC also has a 2+2 cyber security degree with the University of Charleston.

WVU at Parkersburg

The Associate of Applied Science in Computer and Information Technology gives students a foundation in computer hardware and operating systems, and provides hands-on coursework in network administration through Cisco Networking Academy courses, and systems administration through Microsoft Windows and Linux courses. Industry certifications within cyber security include:

- CompTIA Network+
- Cisco CCNA Security Certification

Proposal: West Virginia Community and Technical College System
West Virginia Apprenticeships in Motion (AIM) Program Strategic Plan

West Virginia is now undergoing a diversification and expansion of key business sectors, and one of those is the technology and knowledge-based sector. However, the skills needed for this sector are ones that require specialty and post-secondary education. Recognizing this, policy-makers, state agencies, educational institutions and private entities have developed a workforce solution to meet this industry's requirements and to enable more West Virginia residents to gain the skills to seek employment opportunities in these high tech jobs.

Under the leadership of the West Virginia Development Office and the W.Va. Community and Technical College System, an Apprenticeship in Motion planning team has created and has prepared The West Virginia Community and Technical College System West Virginia Apprenticeships in Motion (AIM) Program Strategic Plan. This plan was built upon the Vision 2020: An Education Blueprint for Two Thousand Twenty (State Code §18B-1D-3), which directed West Virginia's educational institutions to focus on programs which create and retain jobs in the

state especially among the emerging high-technology, knowledge-based businesses and industries.

The implementation of strategies for the ongoing AIM commitment will take a sector-based approach, beginning with Information Technology, as this sector represents some of the best middle-skill career opportunities for West Virginians. The outreach and engagement strategies will be targeted specifically to this sector during year one. At the same time, the systems change envisioned by AIM will not be exclusive to the IT sector. The plan's implementation will enhance the alignment of the workforce system overall, to the benefit of all participating employers and residents.

The work of the Plan will be carried out by the West Virginia Community and Technical College System and will network with workforce and industry partners committed to implementing the systems change and strategies associated with the plan. A $4 million grant application has been submitted to the U.S. Department of Labor that, if approved, would provide funding for this plan.

The Apprenticeships in Motion (AIM) Program will focus on the following objectives:

- Develop and launch a branding campaign that will provide visibility to the comprehensive AIM program and all its connecting parts;
- Cultivate interest in high-demand, high-pay middle skill careers focused on IT and cybersecurity;
- Create awareness within the business community about CTCS' AIM program and how they can take advantage of the West Virginia Learn and Earn program;
- Equip adult students with the skills needed to succeed in the workplace and prepare under-employed individuals to upscale within their current employment space, utilizing an on-the-job-training component in high-demand tech career credential programs;
- Develop responsive curriculum in high-demand tech career pathways (including cybersecurity) that are co-developed with industry partners, data-informed and ensure success and career readiness for students; and
- Ensure statewide alignment of a cohesive, demand-driven education, job skills development, and career training system that focuses on developing and delivering student-centered career pathways.

Projected Outcome

- By 2020, 8,000 additional West Virginian adults will have earned post-secondary credentials through the community and technical college work-based learning programs, **including 1,600 through the AIM - information technology program.**

9. Cybersecurity Education -- K-12

The West Virginia Department of Education has developed a cyber educational plan, which includes curricula and courses that will be available to students in the fall of 2019. These courses will provide a pathway not only to gain knowledge but also to prepare for a cybersecurity industry certification (Security+, CySE+). See Appendix B.

In addition, there are emerging cybersecurity youth programs that are becoming available to young people in West Virginia. These include:

- GirlsGoCyberStart, a free online game of discovery that provides high school girls in West Virginia who are interested in a cybersecurity career with a tool to learn basic cybersecurity skills and test their cyber aptitude;
- CyberPatriots for high school students – http://www.uscyberpatriot.org/;
- Marshall's GenCyber camp for high school students in West Virginia; and
- RCBI's summer cyber education programs for young people.

10. Cyber Development Plan – Military and Veterans

The U.S. Department of Defense updated and issued its 2018 Cyber Strategy, and that document represents the Department's vision for addressing this threat and implementing the priorities of the *National Security Strategy* and *National Defense Strategy* for cyberspace. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Key among the recommendations is one pertaining to cyber workforce development:

> The Department plays an essential role in enhancing the Nation's pool of cyber talent in order to further the goal of increasing national resilience across the private and public sectors. To that end, we will increase our efforts alongside other Federal departments and agencies to promote science, technology, engineering, mathematics, and foreign language (STEM-L) disciplines at the primary and secondary education levels throughout the United States. The Department will also partner with industry and academia to establish standards in training, education, and awareness that will facilitate the growth of cyber talent in the United States.

In West Virginia, the W.Va. National Guard is working to enhance its cybersecurity capabilities. Provided below are a number of recommendations that would complement the WVNG's and state's efforts:

- **Develop Cyber Mountaineer Veterans:** Cyber Mountaineer Veterans would provide veteran with a consolidated resource for information related to cybersecurity opportunities in the state, including cyber education at Community Colleges and four year institutions, information on financial support, and tools to help veteran build a career track in the cyber workforce. Also…credit a database of military and veterans with cyber skills. This would be modeled after a similar program in Virginia: http://cybervets.virginia.gov See more at: https://governor.virginia.gov/newsroom/newsarticle?articleId=19188#sthash.PEWFJjAd.dpuf

- **Cyber Vets Training Program**
  Create a Cyber Mountaineer Veterans training initiative in partnership with offering by the SANS Institute. The offerings would provide veterans another pathway into the cybersecurity workforce via the SANS VetSuccess Immersion Academy. See more: https://governor.virginia.gov/newsroom/newsarticle?articleId=19188

- **WV Cyber Mountaineer Veteran Incentive Program**
  Develop a state tax incentive/credit program to cover moving expenses for veterans and retired military who move to West Virginia and either work or consult on cyber activities. Credit will be provided to companies or firms who hire under the Cyber Mountaineer Veterans program (see #1).

- **WV Cyber Corp Network**
  Have the WVNG and the WVDPMS outline a civilian cyber response network modeled, in part, after the program that has been set up in Michigan - https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html . This network would be designed to enable quick communication/collaboration about major cyber events, facilitate coordinated training activities and provide for a mechanism for affected entities to seek cyber assistance.

- **Incent CyberPatriot Coaches**
  Efforts are underway to expand this program to more schools and students across the state. However, cyber coaches are needed for these new clubs. One idea is to provide paid time off to members of the WVNG who volunteer as coaches for the CyberPatriot Youth Program.

Training Resources

- **NICCS Cyber Training:** https://niccs.us-cert.gov/training/veterans
  - ***FREE training***— veterans can access free cybersecurity training through the Federal Virtual Training Environment (FedVTE).

- **U.S. DHS Cyber Training:** https://www.blogs.va.gov/VAntage/30058/veterans-can-take-advantage-in-free-cybersecurity-training/
  - The Department of Homeland Security (DHS) and Hire Our Heroes have teamed up to offer training for Veterans in cybersecurity, in support of Veterans join our nation's cybersecurity workforce.
  - DHS's Federal Virtual Training Environment (Fed VTE) offers free online, on-demand cyber security training to government employees and Veterans. Veterans can sign up for an account through the Hire Our Heroes website and follow instructions through "ID me" to verify veteran status and register for a FedVTE account.

11. Cyber Education Resources

There are a diverse variety of web sites and on-line resources regarding cybersecurity education and workforce training. Among these are:

a. NIST Cyber Resources - https://www.nist.gov/topics/cybersecurity

b. National Initiative for Cybersecurity Education - https://www.nist.gov/itl/applied-cybersecurity/nice

c. NICE Cybersecurity Workforce Framework: Categorizing and Describing Cybersecurity Work for the Nation: Special Publication 800-181 (Attached) https://www.nist.gov/news-events/news/2017/08/nist-publishes-nice-cybersecurity-workforce-framework-categorizing-and
   NICE – National Institute for Cybersecurity Education - https://www.nist.gov/itl/applied-cybersecurity/nice
   i. Cyber career pathway info -https://www.cyberseek.org/pathway.html

d. USDHS NICCS Educational Resources:
   i. Cybersecurity Workforce Planning Diagnostic (PDF) – *see workforce planning section*
   ii. Students' Guide to Cybersecurity Careers (PDF)
   iii. Teachers' Guide to Engaging Students in Cybersecurity (PDF)

e. NICCS Education and Training Catalog - https://niccs.us-cert.gov/training/search

f. Cybersecurity Supply/Demand Heat Map http://cyberseek.org/heatmap.html

g. National CyberWatch Center's Curriculum Standards (NCC-CSP) https://www.nationalcyberwatch.org/programs-resources/curriculum/

h. NSA/DHS National Centers of Academic Excellence in Cyber Defense https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

i. State cyber strategic proposals - http://www.govtech.com/data/Boosting-the-Cyberworkforce.html?mc_cid=6056097651&mc_eid=629541aaa5

j. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance
   https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6005833/

Also, many states are developing and implementing cybersecurity learning and training programs. See a listing provided by the National Governors Association (See Appendix C)

12. Cybersecurity Workforce Strategic Plan - Recommendations

1) Establish a WV Cyber Education/Training Collaboration Consortium in order to increase the number of individuals being trained in cybersecurity, avoid/pre-empt direct competition among institutions, aid overall collaboration to generate positive external equity and open up added public-private funding opportunities. If done effectively, West Virginia can become one of the nation's leaders in cybersecurity education through offering a rich portfolio of distinct programs across our institutions.

2) Work the with state's congressional delegation to seek federal funding from agencies, such as the U.S. Department of Homeland Security, to establish a pilot project that would create a statewide Cyber Center of Excellence in West Virginia.

3) Work with West Virginia institutions of higher education to become part of a federal cyber scholarship program: US OPM https://www.sfs.opm.gov/.

4) Work with West Virginia institutions of higher education to become part of the U.S. DOE's Cyberforce Competition program: https://cyberforcecompetition.com/. Possibly link with the NETL.

5) Consider utilizing WVNET's PEAK professional development portal as a medium for state-wide training opportunities.

6) Task WVNET to investigate the cost and resources involved in creating virtual labs/machines for K-12 and higher education.

7) Prepare a funding proposal for the FY 2019-20 state budget that provides additional dedicated resources to grow the cybersecurity capabilities of the state's four-year institutions:
   i. More professional development resources/funds are needed at Fairmont State to ensure faculty and trainers are recruited, retained and skilled
      1. Various resources are needed to fully realize the needed capabilities such as:
         a. Upgraded computer labs - $500,000
         b. Cybersecurity software packages for the class rooms and labs - $250,000
         c. Faculty support - $250,000
   ii. To better serve the Marshall's students and strengthen the academic program, additional resources will be needed to obtain two components:
      1. *Academic Partnership*
         Partnership with entities providing certification in cybersecurity to allow students to have better access to the testing materials and reduce the fee to take the certification. Becoming an academic partner of CompTIA and EC-Council, for example, will allow students to have access to several of the in-demand cybersecurity certifications at a significantly reduced price.
      2. *Equipment and Maintenance of Facility*:
         To properly utilize the existing infrastructure built into the networking and cybersecurity lab, the lab will need to be furnished with software and hardware that can emulate various cyber infrastructures that are currently used in the field. In addition, to ensure that such software and hardware are properly deployed and maintained, a lab administrator will need to oversee the day-to-day operation of the lab for both academic and scholarly activities.
   iii. To continue the expansion of Marshall's cyber and digital forensics programs, expanded funding resources also would help provide:
      1. Additional lab, teaching space and equipment.

2. Development and creation of more practical, hand-on lab exercises, case simulations, table top exercises, and the like.
3. More applied research (i.e. costs of consumer products, software, tools, etc.).
4. Student and faculty activities outside the university (conferences, etc.).
5. Administrative assistance to help manage the NSA/DHS CAE program paperwork.

iv. To provide for the high-quality instruction envisioned for experiential and hands-on cybersecurity learning, combined with training in research/thought leadership and continuing/executive education, the state's colleges and university will need added investment in personnel and infrastructure in order to grow and nurture a robust pipeline of cybersecurity talent in WV. The state's programs will require additional resources to fully address the pent up demand and to meet the rapidly emerging employment opportunities. At WVU, the addition of three new faculty lines in each program (total 6 new lines) would significantly accelerate the program development, allowing WVU to leverage existing cybersecurity expertise and our growing industrial and federal partnerships, and to utilize NSA Center of Excellence designations in order to become a regional powerhouse for interdisciplinary cybersecurity education and research. Furthermore, there is significant ancillary benefit to WV by aligning the research efforts of these new hires with regional business priorities. This provides routes to externally funded projects supported by SBIR/STTRs with concomitant economic development opportunities. These new investments in essential faculty require salary and benefits support at the level of $750K/yr.

In addition to personnel, state-of-the-art programs call for on-campus cybersecurity labs that provide "sandbox" infrastructure to permit simulated cyberattacks, that are as realistic as possible, but that do not compromise functioning university systems. These facilities allow for the hands-on learning that employers expect. Such laboratories consist of a network of devices, including a variety of PCs, as well as mobile devices and industrial controllers, which reflect the assortment of information infrastructure that is subject to cyber attacks. The devices are networked behind a hardware router and firewall to separate them from the university computing network, and allow flexible experimentation for both teaching and research. The sandbox should also include the capability to simulate a larger virtual network of machines in a cloud-environment such as Amazon Web Service, to prepare students for realistic network scenarios. The infrastructure would require a one-time capital investment of $300K and need the supervision of a paid full-time Teaching Associate with IT experience at the rate of $75K/yr including benefits.

These investments at a critical juncture in the development of the WVU Cybersecurity programs will fast track the programs to provide maximum benefit and opportunity to both WV students and the our growing cybersecurity economy.

8) Enact a new state tax development incentive that would provide high-technology companies a rebate (up to 10%) of payroll taxes for 5 years. Rebate dollars could be used for either capex OR opex. Eligible high-technology companies would be those engaged in one of the following: applications development, coding, e-commerce services, game development, data analytics, cloud services or cybersecurity.

9) Explore e-learning and tele-learning best practices for the support and management of online learning and online adjunct faculty teaching cyber security.

10) Leverage the West Virginia Cyber Education/Training Collaboration Consortium and added state resources to help develop more cyber internship programs. Also consider the development of a Governor's Cyber Internship Program and grants, and an annual Governor's Cybersecurity School during the summer for high school students.

11) Focus cyber education programs and curricula that address these key employment areas:

- Network operations
- Systems administration
- Cyber monitoring and incident response
- Vulnerability assessment analyst
- Policy development, implementation and adherence

12) Support the W.Va. Dept. of Commerce's and West Virginia Community and Technical College System's $4 million grant application to the U.S. Department of Labor that, if approved would provide funding for The Apprenticeships in Motion (AIM) Program. This community college program would focus on the following objectives:

- Develop and launch a branding campaign that will provide visibility to the comprehensive AIM program and all its connecting parts;
- Cultivate interest in high-demand, high-pay middle skill careers focused on IT and cybersecurity;
- Create awareness within the business community about CTCS' AIM program and how they can take advantage of the West Virginia Learn and Earn program;
- Equip adult students with the skills needed to succeed in the workplace and prepare under-employed individuals to upscale within their current employment space, utilizing an on-the-job-training component in high-demand tech career credential programs;
- Develop responsive curriculum in high-demand tech career pathways (including cybersecurity) that are co-developed with industry partners, data-informed and ensure success and career readiness for students; and
- Ensure statewide alignment of a cohesive, demand-driven education, job skills development, and career training system that focuses on developing and delivering student-centered career pathways.

13) Develop and fund an ACE (13th year) cybersecurity learning program through the West Virginia Department of Education for recent high school graduates.

14) Develop and host a statewide high school cybersecurity competition and annual event.

15) Continue providing state funds to the West Virginia STEM fund so resources are available to offer mini-grants that will generate the creation of more youth cyber activity programs.

16) Encourage more special programs focused on girls and women to consider cybersecurity as a career choice and field.

17) Develop informational resources to share with students who are interested in pursuing careers in cybersecurity so they understand other key non-education requirements:

- Good credit history
- Appropriate personal behaviors and activities
- No criminal record
- Awareness of critical thinking and soft skills

18) Develop a speaker forum of cyber specialists and employers who could meet with students.

19) Below are a number of cyber recommendations that would complement the West Virginia National Guard's cybersecurity capabilities and development efforts:

- Cyber Mountaineer Veterans – The creation of Cyber Mountaineer Veterans would provide veterans and military personnel with a consolidated resource for information related to cybersecurity opportunities in the state, including cyber education at Community Colleges and four-year institutions, information on financial support, and tools to help veteran build a career track in the cyber workforce. Also…credit a database of military and veterans with cyber skills. This would be modeled after a similar program in Virginia: http://cybervets.virginia.gov See more at: https://governor.virginia.gov/newsroom/newsarticle?articleId=19188#sthash.PEWFJjAd.dpuf
- Cyber Vets Training Program - Create a Cyber Mountaineer Veterans training initiative in partnership with offering by the SANS Institute. The offerings would provide veterans another pathway into the cybersecurity workforce via the SANS VetSuccess Immersion Academy. See more: https://governor.virginia.gov/newsroom/newsarticle?articleId=19188
- WV Cyber Mountaineer Veteran Incentive Program - Develop a state tax incentive/credit program to cover moving expenses for veterans and retired military who move to West Virginia and either work or consult on cyber activities. Credit will be provided to companies or firms who hire under the Cyber Mountaineer Veterans program (see 1).
- WV Cyber Corp Network - Have the WVNG and the WVDPMS outline a civilian cyber response network modeled, in part, after the program that has been set up in Michigan - https://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html . This network would be designed to enable quick communication/collaboration about major cyber events, facilitate coordinated training activities and provide for a mechanism for affected entities to seek cyber assistance.
- Incent CyberPatriot Coaches - Efforts are underway to expand this program to more schools and students across the state. However, cyber coaches are needed for these new clubs. One idea is to provide paid time off to members of the WVNG who volunteer as coaches for the CyberPatriot Youth Program.

Other

- Support WVForward's exploration and study effort into how to develop a better, clearer security clearance process for individuals who want to pursue employment in cybersecurity fields. This may involve a sequence of steps to help facilitate easier and faster entry-level employment and then continue with low-cost ways for individuals to get necessary clearances in order to advance.
- Develop new educational programs and degrees that focus on cybersecurity policy. Programs are needed across the country that produce graduates capable of answering questions such as:
    - What existing policies address pressing cybersecurity threats? Where are there gray areas exploitable by malicious actors?
    - Who has jurisdiction when a major cybersecurity attack occurs?
    - What redundancies, contradictions, and gaps are revealed when examining local, state, and federal cybersecurity policy?

  Source: https://www.wilsoncenter.org/sites/default/files/cybersecurity_workforce_preparedness.pdf
- Create a central web portal that will share information on cyber learning programs across the educational continuum as well as list job opportunities, resume postings, internships, sanctioned cyber competitions, etc.

13. Related Efforts

- **WVForward Security Clearance Roundtable**
  WVForward is spearheading a roundtable discussion and work group to analyze the issues associated with the backlog of security clearances nationwide, and to explore how this creates challenges and inhibits job growth for many West Virginia industries, including cybersecurity and federal tech contractors.

- **WVSBDC Cyber Threat Awareness Initiative**
  The West Virginia Small Business Development Center has created two new cybersecurity resources for the state's small business community:
  - The Small Business Big Threat assessment web site is available at www.smallbusinessbigthreat.com/west-virginia. The "*Small Business Big Threat*" online course is designed to increase business owners' cybersecurity awareness of threats, prevention and response. The assessment enables business owners to test what they know, review best practices and identify a cybersecurity action plan for their businesses. Suitable for both cyber-savvy and nontechnical owners, the course presents lessons learned from the experience of other small businesses. In the "cybersecurity challenge," the business owner pits his or her knowledge against cyber villains who attack through weaknesses such as data protection, passwords and physical security. Participants who complete the program receive a free Cybersecurity Readiness Checklist.
  - The SBDC "*Small Business Big Threat"* cybersecurity workbook (see attachment or download from the Resources page at www.wvsbdc.com). The booklet includes identification of the most common methods of cyber breaches, the National Institute of Standards and Technology five-part framework to reduce the risk of a cyberattack, cybersecurity tips for small businesses and additional resources.

- **WV Manufacturing Extension Partnership**
  The West Virginia Manufacturing Partnership (WVMEP) provides multiple services to small businesses in the area of Cyber Security. Firstly, they partner with cyber security experts from the National Institute of Standards and Technology (NIST) which is the parent organization of the national MEP program, to provide educational workshops on the types, breadth, and depth of the cyber threats. During these workshops the attendees see and hear how the attacks occur, what information the attackers are seeking, and methods to prevent and/or slow down the attacks. Also, there is an overview of the cyber security standards required to do business with the DoD, and general best practices for all businesses. Secondly, the WVMEP has developed a Cyber Security assessment that small businesses can easily understand and utilize to evaluate their level of security and identify weaknesses. This assessment was developed from the NIST Cyber Security assessments and was designed to be a low level evaluation. And finally, the WVMEP will help our clients evaluate the assessment to determine if they need to retain a Cyber Security expert that can do a more detailed assessment and provide countermeasures to the weak areas and ongoing support. The WVMEP has identified qualified experts that provide Cyber Security services in West Virginia.

14. 2019 Activities

Provided are activities planned for 2019 as a continuation of this strategic planning process:

- Quantify Cyber Employment Needs, Opportunities in West Virginia

- Outreach and Awareness Plan
    - WVU, Marshall alumni and students
    - West Virginia business community
    - West Virginia media

- Link with cyber outreach and recruitment plan being developed to focus on military and veterans
    - WV National Guard

Appendices

A. List of participants on W.Va. Cybersecurity Workforce Strategic Planning Group

B. W.Va. Department of Education Cyber Education Plan

C. NGA Report on State Cyber Workforce Initiatives

WV Cybersecurity Workforce Working Group

Anne	Barth	TCWV	anne@techconnectwv.org
Larry	Malone	Malone Consulting & Strategies	lmalone@malonecs.com
4-Year			
Matt	Turner	HEPC	mturner@hepc.wvnet.edu
Mary	Stewart	WVNET	mstewart@mail.wvnet.edu
Harmony	Garletts	WVNET	hgarletts@mail.wvnet.edu
John	Maher	Marshall University	maherj@marshall.edu
John	Sammons	Marshall University	john.sammons@marshall.edu
Bill	Gardner	Marshall University	bill.gardner@marshall.edu
Terry	Fenger	Marshall University	fenger@marshall.edu
Wook-Sung	Yoo	Marshall University	yoow@marshall.edu
Paulus	Wahjudi	Marshall University	wahjudi@marshall.edu
Wael	Zatar	Marshall University	zatar@marshall.edu
Martin	Roth	University of Charleston	martinroth@ucwv.edu
Michael	Levy	University of Charleston	michaellevy@ucwv.edu
John	Barnette	University of Charleston	johnbarnette@ucwv.edu
Matthew	Gonzalez	University of Charleston	matthewgonzalez@ucwv.edu
EK	Esawi	University of Charleston	eesawi@ucwv.edu
Matt	Harbaugh	WVU	Matt.Harbaugh@mail.wvu.edu
Katerina	Goseva	WVU	katerina.goseva@mail.wvu.edu
Mark	Gavin	WVU	mark.gavin@mail.wvu.edu
Virginia	Kleist	WVU	Virginia.Kleist@mail.wvu.edu
Sheena	Murphy	WVU	sheena.murphy@mail.wvu.edu
Larue	Williams	WVU	Larue.Williams@mail.wvu.edu
Brian	Woerner	WVU	Brian.Woerner@mail.wvu.edu
Priscila	Santos	WVForward	priscila.santos@mail.wvu.edu
Josh	Cook	WVForward	joshua.cook3@mail.wvu.edu
Rocky	Goodwin	WVForward	ragoodwin@mail.wvu.edu
Marcus	Fisher	Fairmont State	mfisher13@fairmontstate.edu
Todd	Clark	Fairmont State	Todd.Clark@fairmontstate.edu
Mirta	Martin	Fairmont State	Mirta.Martin@FairmontState.edu
Tom	Devine	Fairmont State	tdevine1@fairmontstate.edu
Joan	Propst	Alderson Broaddus	propstjl@ab.edu
Michael	Boehke	Alderson Broaddus	boehkemj@ab.edu
Atef	Shalan	Alderson Broaddus	shalanam@ab.edu
Lisa	Reilly	Bethany College	LReilly@bethanywv.edu
Naveed	Zaman	WV State University	zamanna@wvstateu.edu
Ted	Lewis	Bluefield State	tlewis@bluefieldstate.edu
Dave	Carrick	WVU Industrial Extension-WV Manufacturing Extension Partnership	David.Carrick@mail.wvu.edu
Gary	Hampton		GaryWayneHampton@gmail.com

WV Cybersecurity Workforce Working Group

WV Govt.			
Ashley	Summit	Governor's Office	Ashley.E.Summitt@wv.gov
Jordan	Damron	Governor's Office	Jordan.L.Damron@wv.gov
Jeff	Vandall	WV Development Office	Jeffrey.W.Vandall@wv.gov
Josh	Spence	Office of Technology	Joshua.D.Spence@wv.gov
Jody	Ogle	WV National Guard	jody.w.ogle.mil@mail.mil
Sallie	Milam	WV Privacy Officer	Sallie.H.Milam@wv.gov
Debra	Martin	WVSBDC	Debra.K.Martin@wv.gov
C&TC			
Sarah	Tucker	WVC&TC	tucker@wvctcs.org
Nancy	Ligus	WVC&TC	ligus@wvctcs.org
Bob	Hayton	BridgeValley C&TC	bob.hayton@bridgevalley.edu
Matthew	Demaria	Pierpont C&TC	matthew.demaria@pierpont.edu
Rob	Linger	Pierpont C&TC	Rob.Linger@Pierpont.edu
Mary	Butler	New River C&TC	mbutler@newriver.edu
Jerry	Wallace	New River C&TC	jwallace@newriver.edu
Wendy	Patriquin	New River C&TC	wpatriquin@newriver.edu
Gary	Thompson	WVU-P C&TC	gary.thompson@wvup.edu
Stephen	Smoot	Eastern C&TC	stephen.smoot@easternwv.edu
K-12 Education			
Kathy	D'Antoni	WV Dept. of Education	
Lori	Whitt	WV Dept. of Education	lwhitt@k12.wv.us
Tim	Elliott	WV Dept. of Education	tbelliott@k12.wv.us
Ameilia	Courts	Education Aliance	amelia@educationalliance.org
Todd	Ensign	NASA/WV Robotics Alliance	todd.i.ensign@nasa.gov

WV Cybersecurity Workforce Working Group

Industry			
Jim	Estep	WV High Tech Foundation	jestep@wvhtf.org
Steve	Morris	IBM	Stephen.L.Morris@ibm.com
Martin	Laird	IBM	lairdmar@us.ibm.com
Craig	Bury	Retired (IBM)	craig.bury@rcn.com
James	Sharpe	CSRA	James.Sharpe@csra.com
Jeff	Tucker	Leidos	Jeffrey.Tucker@leidos.com
Rebecca	Hall-Herndon	NOAA	rebecca.hall-herndon@noaa.gov
Jeffery	Bowmar	US Dept. of Commerce	jbowmar@doc.gov
Daniel	Bollinger	NOAA	daniel.bollinger@noaa.gov
Richie	Wilbur	Advantage Tech	rwilbur@advantagetech.biz
Rob	Dixon	Advantage Tech	rdixon@advantagetech.biz
Jack	Shaffer	Advantage Tech	jshaffer@advantage.tech
Timi	Hadra	IBM	thadra@us.ibm.com
Trey	Clark	IBM	tclark@us.ibm.com
Cecelia	Schartiger	IBM	schartig@us.ibm.com
Brian	Moats	MPL	bmoats@mpl.com
Brian	Stolarik	Northrop Grumman	Brian.Stolarik@ngc.com
Norm	Gundersen	Global Science and Tech	norman.gundersen@gst.com
Glenn	Copen	Key Logic	gcopen@keylogic.com
Edward	Abraham	FBI/CGIS	elabraham@fbi.gov
Greg	Blaney	NASA IV&V	Gregory.D.Blaney@nasa.gov
Ken	Rehm	NASA IV&V	Kenneth.D.Rehm@nasa.gov
Donald	Ohl	NASA IV&V	Donald.C.Ohi@nasa.gov
Liam	Bowers	Blue Stone Analytics	lbowers@bluestoneanalytics.com
Lindell	Alderman	F5 Networks	lindell.alderman@gmail.com
Jason	Rolleston	McAfee	jrolleston78@gmail.com
Karen	Goodwin	Service Members Opportunities Colleges	karen.goodwin@us.ibm.com
Jim	Spencer	City of Bluefiled	jspencer@cityofbluefield.com
Gerard	Eldering	InnovateTech Ventures, LLC	gerard@innovatetech.com
John	Sedoski	National White Collar Crime Ctr.	JSedoski@nw3c.org
Ryan	Thorn	Senator Manchin's Office	Ryan_Thorn@manchin.senate.gov
Aaron	Sporck	Senator Capito's Office	Aaron_Sporck@capito.senate.gov

1900 Kanawha Boulevard, East, Building 6 • Charleston, WV 25305
wvde.us

WV Cyber Workforce Plan - WVDE Component

The West Virginia Department of Education is committed to providing cyber security preparation to WV students in both K-12 and in Career and Technical Education. The WVDE plan includes an assessment of current policies related to cyber security in K-12, teacher resources and professional development related to cyber security, club and camp activities for students related to cyber security, and a commitment to developing new academic opportunities for students in cyber security. In CTE, the cyber security pathway is clearer, and information related to those programs are included in this plan.

Reaching students with the issues and practices related to cyber security needs to begin in the elementary grade levels, so that students are prepared to understand the problems and solutions related to cyber security as they enter middle- and high-school and become true digital users and producers.

Assessment of current policies related to Cyber Security

Policy 2520.15 contains the West Virginia College- and Career-Readiness Standards for Technology and Computer Science. The language of these standards describes security and privacy as a component of Computer Science, and thus is required to be taught by WV K-12 teachers. “Computer science has a wide range of specialties. These include computer architecture, software systems, programming and coding, graphics design, music technology, robotics & artificial intelligence, web design, security & privacy, computational science, and software engineering. Drawing from a core of computer science knowledge, each specialty area focuses on particular challenges.”

In K-2, the focus is more related to Digital Citizenship.

Digital Citizenship	
TCS.K-2.15	Demonstrate responsible use of technology (i.e., seek guidance and appropriate support when selecting digital content, understand how to be safe online, follow safety rules when using media, etc.).
TCS.K-2.16	Practice using safe, legal, and ethical behavior when using technology.

In 3-5, the focus is still on Digital Citizenship, but deepens to include topics such as online identities, appropriate online interactions, and the importance of keeping personal data private.

Digital Citizenship	
TCS.3-5.20	Practice using safe, legal, and ethical behavior when using technology and interacting online.
TCS.3-5.22	Demonstrate an understanding of the role an online identity plays in the digital world and learn the permanence of decisions made when interacting online.
TCS.3-5.23	Demonstrate appropriate methods of sharing personal data online and how to keep personal data private.

With the move to Middle- and High-School, Digital Citizenship again deepens and begins to include an introduction to Cyber Security which includes, but it not limited to standards such as:

TCS.6-8.16	Demonstrate an understanding of what personal data is and how to keep it private and secure, including the awareness of terms such as encryption, HTTPS, password, cookies and computer viruses; they also understand the limitations of data management and how data-collection technologies work.

And

TCS.9-12.16	Keep personal data private and secure, including the awareness of terms such as encryption, HTTPS, password, cookies and computer viruses; understand the limitations of data management and how data-collection technologies work.

In middle- and high-school, however, students also begin to take specific courses in Computer Science, which all include some component of cyber security. The current courses listed in policy include:

Middle School: *Discovering Computer Science*
Discovering Computer Science is designed for students in grades 6-8 and will provide them with opportunities to explore the many facets of Computer Science. This may be taught in a single class in one grade level or divided into sections and taught over a three-year period.

Standards related to cyber security:

TCS.DCS.25	Demonstrate good practices in personal information security, using passwords, encryption, and secure transactions.
TCS.DCS.34	Describe the major components and functions of computer systems and networks.
TCS.DCS.37	Demonstrate legal and ethical behaviors when using information and technology and discuss the consequences of misuse.

High School: *Computer Science in the Modern World*
Computer Science in the Modern World is a course designed for all students in grades 9-12 and includes the essential skills that all high school students should have upon graduation.

Standards related to cyber security:

TCS.MW.24	Explain the principles of security by examining encryption, cryptography, and authentication techniques.
TCS.MW.35	Explain the basic components of computer networks (e.g., servers, file protection, routing, spoolers and queues, shared resources, and fault-tolerance).
TCS.MW.47	Describe security and privacy issues that relate to computer networks.

High School: *Computer Science & Mathematics*
Computer Science & Mathematics may be counted as a fourth math elective credit course and must be taught by a certified 9-12 math teacher.

Standards related to cyber security:

TCS.M.43	Describe security and privacy issues that relate to computer networks.
TCS.M.44	Explain principles of network security and techniques that protect stored and transmitted data (e.g., encryption, cryptography, authentication).

Standards related to cyber security:

TCS.GIS.20	Demonstrate an awareness of the ethical and social implications of the use of GIS and GPS system, including system reliability, privacy, legal issues, and the social and ethical ramifications of their use.
TCS.GIS.21	Identify the impacts GIS and GPS systems have on individuals, society, commercial markets, and innovation.

Complete standards for these courses can be found in policy at http://wvde.state.wv.us/policies/ .

K-12 Plan – Support for Student Opportunities in Cyber Security

K-2 - Promote Cyber Security Resources for young children such as:

- the literature series from Cyber Patriots that includes pre-K books such as *Sarah the Cyber Hero*
- *Cyber Patriots interactive learning module* Security Showdown 2, geared at K-2 students and teaches students about Personal Information

L-5 - Promote Cyber Security Resources for intermediate children such as:

- *Cyber Patriots interactive learning module,* JeffOS is for grades 3-6 and teaches about phishing, malware and firewalls.
- *Cyber Patriots interactive learning module,* Packet Protector is also geared at grades 3-6 and teaches about malware, defenses and passwords.

M-8 - Promote Cyber Security Resources for secondary students such as:

Cyber Patriots middle school competition (http://www.uscyberpatriot.org/)
GenCyber Camps - https://www.gen-cyber.com/
The Cyber Security Lab – activity found at http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/

9-12 - Promote Cyber Security Resources and courses for secondary students such as Cyber Start -

https://www.sans.org/CyberStartUS/
Girls Go Cyber Start - https://www.sans.org/CyberStartUS/additional-resources
Cyber Patriots high school competition (http://www.uscyberpatriot.org/)
GenCyber Camps - https://www.gen-cyber.com/
The Cyber Security Lab – activity found at http://www.pbs.org/wgbh/nova/labs/about-cyber-lab/educator-guide/

High School Optional Course Offerings Containing Cyber Security Components:

AC Informatics 3 – Database in the Cloud

Fundamentals of Computer Systems
AP Computer Science Principles
Cisco Networking
Networking Essentials
Wireless Networking Essentials
Sercurity +
Server Essentials
Digital Computer Concepts

K-12 Plan – Support for Teachers - Resources and Professional Development in Cyber Security

WVDE will disseminate resources to educators, and will provide opportunities for teachers to receive professional development in cyber security.

Current resources to be distributed include:
Free Resources for Teaching Students about Cyber Security - http://www.oriontech.com/free-resources-teaching-students-cyber-security/

NICCS Educational Resources:
Cybersecurity Workforce Planning Diagnostic (PDF) – *see workforce planning section*
Students' Guide to Cybersecurity Careers (PDF)
Teachers' Guide to Engaging Students in Cybersecurity (PDF)

NICE – National Institute for Cybersecurity Education -https://www.nist.gov/itl/applied-cybersecurity/nice

Cyber career pathway information -https://www.cyberseek.org/pathway.html

US-CERT - the United States Computer Emergency Readiness Team https://www.us-cert.gov/ncas/tips

Potential Future Plans for Developing Academic Opportunities in Cyber Security

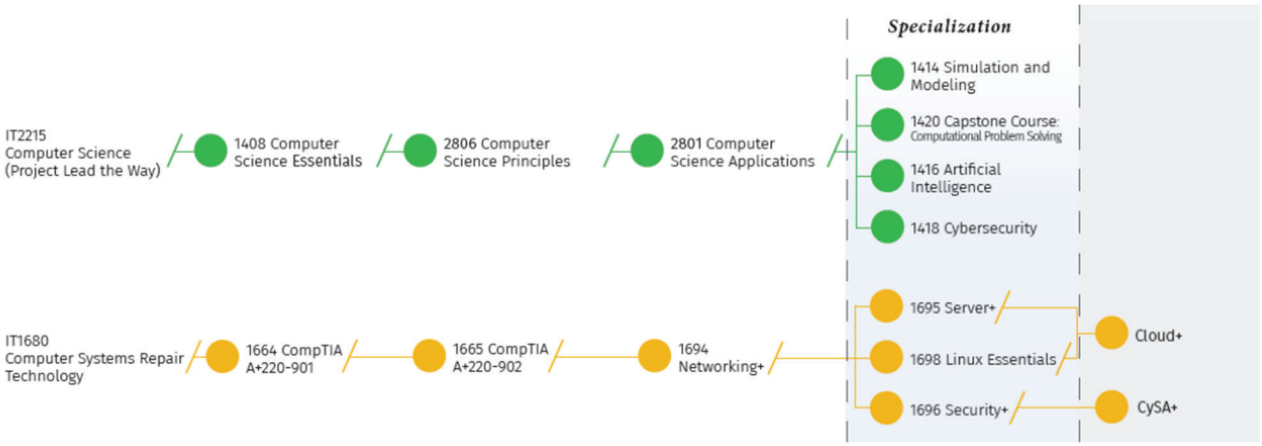
- Develop courses for students via WV Virtual School to fill the gaps due to scheduling conflicts, non-certified teachers, etc.
- Develop training for teachers so they may develop a deeper understanding of cyber security
- Host Cyber Security Camps for students

Career and Technical Education Component

The West Virginia Department of Education Office of Career Technical Education is implementing two programs of studies to meet the needs of the workforce Cyber Security shortage.

- The Project Lead the Way Computer Science program of study will focus on the coding / software side of Cyber Security.
- The Computer System Repair program of study will focus on the hardware / networking aspect of Cyber Security.

These programs offer a sequence of courses that provides coherent and rigorous content aligned with challenging academic standards and relevant technical knowledge and skills needed to prepare for further education and cybersecurity-related careers in the Information Technology career cluster.



National Governors Association Report on State Cyber Workforce Initiatives

State	Initiative	Reference URL	Summary
Virginia			
	Cyber Virginia	https://cyberva.virginia.gov/	Initiative to help create/develop a pipeline of skilled cybersecurity workers to meet the demand of cyber jobs. Through the VA. Cyber Commission, an education-centric approach was developed and included in the Governors budget to increase CAE's, SFS, and other programs to the development of cyber skills and/or capabilities.
	Cyber Initiatives included in 2017-18 Budget bill		Increase Cyber Centers of Excellence, VA scholarship for service, Veterans Pathwar in Cyber Security (GWU); VA Cyber Range, etc.
	CyberCamps	http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybercamps/index.shtml	Through the Virginia Department of Education the CyberCamps program serves as a pipeline for students K-12 to help bring awareness to cybersecurity, focusing on cyber literacy, problem driven projects related to cyber, and cyber opportunities in the workforce. This program involves 32 public schools within 8 regions.
	Adoption of the NICE Framework	https://governor.virginia.gov/newsroom/newsarticle?articleId=21075	The new framework will provide state agencies and educational institutions with a common, consistent lexicon that categorizes and describes cybersecurity jobs by category, specialty area, and work role. It is also a resource for firms and/or industry sectors with shared needs for a cyber workforce. Employers can use the framework to provide guidance for Virginia's workforce education and training partners to support more strategic workforce development efforts statewide.
	Virginia Cyber Security Comission	https://governor.virginia.gov/newsroom/newsarticle?articleId=4817 ; http://www.doe.virginia.gov/instruction/career_technical/cybersecurity/cybersecurity-white-paper.pdf	The VA. Cyber security Commission was establish as part of the Executive order (EO8) and is focused on building public-private partnerships in an effort to help strengthen cybersecurity in Virginia. The responsibilities of the committee are to help identify cyber issues, bring awareness to cyber hygiene, provide recommenations to improve the workforce pipeline, and etc. The committee is comprised of academia, industry, and government.

State	Initiative	Reference URL	Summary
Maryland			
	Maryland Cybersecurity Council	http://www.umuc.edu/visitors/president/maryland-cybersecurity-council.cfm	The Maryland Council was created help improve the cyber standards and practices in Maryland by fostering a common guidance to addressing cybersecurity issues. This council is comprised those in the public and private sector.
	Cyber Maryland		This is a yearly two-day conference that is focused on bringing together thought leaders in academia, industry and government. There are recognized speakers and panelists, break-out sessions on various cyber related topics, cyber job fair, industry showcase of products/services, and a networking social. The purpose is for information sharing and building of collaborations for the development of cyber assets - human and technological.
	CyberWorks	http://www.cyberworksmd.org/	Organization focused on helping build the cybersecurity workforce in Maryland by using a industry led approach. Using an model involving a two-week-sprint, candidates are vetted and screen for a perfect fit for a business. **Funded by State of Maryland's EARNMaryland Grant Program, administered by Marylands Labor, Licensing and Regulation.** http://www.cyberworksmd.org/model.html
Maryland	EARNMaryland	http://www.dllr.state.md.us/earn/	EARN Maryland is a new state-funded, competitive workforce development grant program that is industry-led, regional in focus and a proven strategy for helping businesses cultivate the skilled workforce they need to compete. This program aims to address workforce shortages, establish career paths, and skills development
Indiana			
	Career Makers	https://polytechnic.purdue.edu/anderson/careermakers	CareerMakers is an industry-led workforce education and training program that is addressing the critical workforce development needs of companies, government and agencies located in the State of Indiana and beyond.
	Cyber Academy	http://www.therepublic.com/2018/06/03/cyber_academy_partnership_provides_key_benefits/	Ivy Tech Community College is working collaboratively with the Indiana National Guard to launch a cyber academy.
	Working Groups of the Indiana Executive Council on Cybersecurity	https://www.in.gov/cybersecurity/3822.htm	A focus on various Cybsersecurity related topics. One working group focuses on Workforce Development for building educational programs and pipelines.

State	Initiative	Reference URL	Summary
Texas			
	Texas Cybersecurity Council	http://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=133	The Texas Cybersecurity Council was created by the Department of Information Resource as to establish and develop private-public partnerships. The council focuses on developing stratgies and solutions for building the cyber workforce, promote innovation and collaboration to increase awareness and products to cybersecurity, evaluate program requirements, and etc.
	Cyber Texas	https://www.cybertexas.org/	The CyberTexas Foundation is focused on cyber workforce development, economic development, and preparedness. They hold a conference that help bring together experts in government and private sectors to bring attention to and help address cybersecurity issues.
	National Security Collaboration Center	https://www.xconomy.com/texas/2018/05/08/san-antonio-university-takes-aim-at-gap-in-cybersecurity-workforce/	National Security Collaboration Center, it will be a physical space that aims to be a central gathering place for government agencies and businesses who are seeking both future cybersecurity workers, as well as contemporary research by students that might aid the organizations' existing projects
	(San Antonio) Chamber's Cybersecurity Industry Council Task Force	https://www.sachamber.org/news/2017/08/30/chambers-cybersecurity-council-tackles-issue-around-san-antonios-security-workforce/	The Chamber's Cybersecurity Industry Council, the driving force behind CyberSecurity San Antonio, has launched a new task force that aims to better quantify and promote the talent transitioning out of post-secondary education providers with security skillsets.
Michigan			
	Michigan Cyber Initiative 2015	https://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf	Michigan Cyber Initiative is focused on people, policy, and technology to address cybersecurity issues and concerns. This public-private partnership looks to develop ongoing efforts for education and cyber awareness, Cyber industry opportunties, and building a cyber ecosystem for a more holistic approach.
		http://www.michigan.gov/cybersecurity/	

State	Initiative	Reference URL	Summary
California			
	CyberCalifornia	http://cybercalifornia.biz/	Initiative that supports and helps to promots the California Cybersecurity Task Force by helping to foster connections between public and private institutions with the goal of encouraging innovation, education, and workforce development. In connection with this is iHubs with is a innovatine platform administered by Governor's Office of Business and Economic Developement.
	Cybersecurity Task Force	http://www.caloes.ca.gov/for-individuals-families/cybersecurity-task-force	Directed by Gov. Jerry Brown, the California Cybersecurity Task Force was created to help foster and promote a culture of cybersecurity through education, information sharing, workforce development and economic growth. The task force has 8 goals that support the building of California's cybersecurity position and resiliency. To achieve these goals, the Task Force is made up of 7 committees that are comprised of volunteers from industry, academia, and government.
	Hi Tech Initiative - TechEd	http://www.bixelexchange.com/tech_ed_partnerships	Bixel Exchange in partnership with LA HI-Tech, helps to bridge the skills gap by connecting industry and academia. Through mentorships, tours, hackathons, internships, and classroom visits students are provided with formal and informal educational opportunties. Currently, there are 8 community colleges, 30 high schools, and 4,000+ students. This sponsored by the LA Chamber of Commerce.
	LA Chamber of Commerce Recruitment and Training Strategy by Bixel Exchange		Bixel Exchange won a contract with LA to provide Recruiting and Training strategies with a focus on number of jobs, best practices, awareness, case management, and building connections. Th areas of interest are IT, Logistics, Manufacturing, and Biotech. **This is still being developed**
Florida			
	Supervisors of Elections Training and Key Personnel	https://news.uwf.edu/university-of-west-florida-partners-with-state-and-local-election-officials-to-enhance-cybersecurity-preparations/	The University of West Florida Center for Cybersecurity recently partnered with the Florida Department of State and election officials across Florida to provide training for supervisors of elections and key personnel to enhance cybersecurity resiliency ahead of the 2018 elections.
	Florida Center for Cybersecurity (FC2)	http://thefc2.org/	The Florida Center for Cybersecurity is a shared resource for academia, government, and industry to help expand educational offerings, increase research capabilities, and and foster partnerships to address cybersecurity. This state initiative is focused on creating more jobs, enhancing the cybersecurity workforce, bringing more innovation, and being a hub for the community.

State	Initiative	Reference URL	Summary
Maine			
	Maine Cybersecurity Cluster (MCSC)	http://maine-cyber-security.github.io/	The Maine Cyber Security Cluster (MCSC) is an academic and research center bringing together government, industry, and academia dedicated to workforce and economic development in the field of cyber security. Its focus is project oriented that involves students experimenting and being innovative with cyber related actitives, helping them gain practical experience. They have stimulations, various tools for project development, and resources - IT professionals.
	Student projects	http://maine-cyber-security.github.io/what-we-do/student-projects/	
North Carolina			
	iCenter	https://icenter.nc.gov/	iCenter is a innovative center created by the NC Department of Information Technology to promote strong collaborations and connect academia, government, and industry, for developing technologies, provide training capabilities for state employees, information sharing, and etc. The vision of iCenter is to provide a simple way to interact with government and develop technology solutions in a creative way.
North Dakota			
	Cybersecurity and Computer Networks Program	https://www.nd.gov/itd/news/5834/north-dakota-and-palo-alto-networks-collaborate-cybersecurity-education	North Dakota Gov. Doug Burgum, Chief Information Officer Shawn Riley and Bismarck State College (BSC) President Dr. Larry Skogen announce an educational collaboration with Palo Alto Networks that will grow the college's Cybersecurity and Computer Networks Program.
Arizona			
	Workforce pipeline for Cybersecurity at EMCC - DoL Grant	https://www.estrellamountain.edu/programs/cybersecurity	To help reduce this critical workforce shortage, the Arizona Sun Corridor-Get Into Energy Consortium (ASC-GIEC), which received a $13.5 million Department of Labor (DOL) grant to advance the training and development of a workforce pipeline for the energy industry, is creating an energy-related cybersecurity program through Estrella Mountain Community College (EMCC), the consortium's lead institution.
Oklahoma and surrounding states			
	Cyber security Education Consotium (CSEC). Formally known as Oklahoma Center for Information Assurance and Forensics Education.	https://atecenters.org/st/csec/	CSEC is a cohesive partnership of community colleges and career and technology centers in Oklahoma, Arkansas, Colorado, Kansas, Louisiana, Missouri, Tennessee and Texas and the University of Tulsa, which serves as the principal training entity and mentor to the two-year institutions. **Funded by a NSF grant**

State	Initiative	Reference URL	Summary
Colorado			
	House Bill 16-1453 signed by Gov. John Hickenlooper	http://pressreleases.uccs.edu/?p=2851	Identifies Colorado Springs as the location for the National Cyber Intelligence Center to respond to cyber-attacks, to train government and private sector leaders to respond to them, and to do workforce development and research. The bill supports a partnership of academics at UCCS and other higher educational institutions to leverage military, state, federal, local government as well as private sector resources.
Delaware			
	Delaware Cyber Aces (SANS)	http://news.delaware.gov/2013/09/10/governor-launches-delaware-cyber-aces-program/	Delaware Cyber Aces targets high schoolers, college students, veterans, and jobseekers in an effort to identify and develop top talent.
	UD Cybersecurity Initiative	https://csi.udel.edu/mission-statement/	The Cybersecurity Initiative (CSI) was established in 2014 as a partnership among the state, University of Delaware, federal agencies, and the private sector to address a problem that costs billions of dollars a year through education, training, and research.
Missouri			
	Missouri Governor's Cybersecurity Summit Initiative)	http://www.govtech.com/events/Missouri-Governors-Cybersecurity-Summit.html#/overview	Currently a yearly summit that focuses on engaging public, private, and academia for Information Sharing, Training/ Exercises, Workforce Development, Hardening Critical Infrastructure, and Incident Response. **Two topics that are very relevant to NICE is "solving the personnel gap" and "the role of education in cybersecurity."**
		https://www.mosheriffs.com/gov-nixon-announces-statewide-cybersecurity-preparedness-initiative/	
New Mexico			
	Center for Cyber Defenders	http://www.sandia.gov/careers/students_postdocs/internships/institutes/cyber_defenders.html	Program to train cyber defenders who can move into computer security jobs at Sandia. Learn to combat cyberattacks, while gaining practical experience in understanding computer systems, network operations, and information protection.CCD interns are part of a Sandia program, Technical Internships to Advance National Security (TITANS),
	Western Cyber Exchange (Colorado, New Mexico, and Wyoming)	http://www.wcyberx.org/wcx-rmta	Public-Private partnership (including DHS, MITRE, and Advanced Cyber Security Center - ACSC) that focuses on security of the cyber domain for communities and industry within the critical infrastructure through the sharing of threat intelligence and data, education and training for workforce development, and supporting the advancement of cyber related technology through research and development activity.
New York			
	New York State Cyber Security Conference and Symposium on Information Assurance	https://www.its.ny.gov/eiso/19th-annual-cyber-security-conference	Northeast conference for cyber security education, the event is co-hosted by the New York State Office of Information Technology Services, the NYS Forum, Inc., and the University at Albany's School of Business.

State	Initiative	Reference URL	Summary
Massachusetts			
	Mass. Skills Capital Grant Program	http://www.mass.gov/edu/government/executive-office-of-education/grant-information/massachusetts-skills-capital-grant-program-.html	The Skills Capital Grant Program awards grants to support vocational/technical training, upgrades and expansion of career technical education, and training of high-quality career pathway programs that are aligned with regional economic and workforce development priorities for in-demand industries, such as Information Technology.
Connecticut			
	Cyber Security Strategy	http://portal.ct.gov/-/media/Office-of-the-Governor/Connecticut-Cybersecurity-Resource-Page/Connecticut-Cyber-Security-Strategy.pdf?la=en	High level main points: more collaboration with businesses and higher education institutions, more communication with executive leadership, HR change for better recruitment, and more matching of cybersecurity demands with training and personnel resources
Georgia			
	Hull McKnight Georgia Cyber Center for Innovation and Training	https://gta.georgia.gov/hull-mcknight-georgia-cyber-center-innovation-and-training	A state-owned facility designed to promote modernization in cybersecurity technology for both the private and public sectors through unique education, training, research, and practical applications.
	Cybersecurity Workforce Academy	https://gta.georgia.gov/georgia-cybersecurity-workforce-academy	Provide cybersecurity awareness, training, and education. Will take place in the Hull McKnight Georgia Cyber Center for Innovation and Training
Vermont			
	Workforce Growth Initiatives	http://governor.vermont.gov/press-release/governor-phil-scott-appoints-degree-and-buxton-lead-workforce-growth-initiatives	Focused on increasing the WF. There is a Workforce Development Board, a 58-member panel charged with coordinating workforce training and education programs and engaging the state's employers, workers and other partners.


CYBERSECURITY

FOR MORE INFORMATION CONTACT:

TECHCONNECT
WEST VIRGINIA

www.techconnectwv.org