Collaboration & Diversity:

Virginia's Winning Strategy for Cyber Security Leadership

Four decades ago, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF) profoundly changed the direction of the world in the creation and support of the internet. Both institutions call Virginia home, and with good reason. By incorporating principles of collaboration, coordination, government involvement and investment, and integration across key markets, Virginia has created the best environment for cyber security research and development in the United States.[1]

Policymakers in the Commonwealth were early to recognize that cyber security would be paramount in the protection, and basic supportive enabling technology, for the next generation economy. Technology, they agreed, does not exist or evolve in a vacuum, but relies on connection, innovation, and legislative understanding and development. By leading the nation in the adoption of industry best practices, Virginia is a nationally recognized trailblazer that has consistently served as a both a driver and early adopter of the best cyber security technologies available.[2]

Today, the Commonwealth of Virginia is home to the most cyber security firms east of the Rockies and has developed a world leading technology ecosystem founded on private industry innovation and public-private partnerships. Thousands of Virginians work on cyber security every day in firms, universities and colleges, the military, the intelligence community, and Commonwealth agencies.

The Commonwealth of Virginia continues to drive the development of new products, companies and services in the cyber security industry, underscored by its unique and abundant technology resources and leadership throughout the United States. As the Commonwealth moves forward, its vision is not only to continue to lead the nation in the adoption of signature Information Communication Technologies (ICTs), but to help formulate and promote their creation through innovation, investment, and a pro-business environment that nurtures all companies.

New cyber security companies, built on the solutions derived from highly advanced and technical research at supported institutions, universities, and collaborations between the defense industry and private firms, are meeting the challenges posed by the ever more interconnected world. The principle of integrated leadership is at the root of this economic success story. Virginia policymakers at the local, state, and federal levels enable business, government, and education organizations to rise to the challenges together, and in collaboration. This environment that nurtures technology growth has encouraged the top cyber security companies to relocate to the Commonwealth and has culminated in Virginia receiving the greatest amount of federal investment for cyber security in the nation.

There are several unique qualities that make Virginia the ideal place to work on cyber security problems. First, a shared vision for pro-business policies and incentives across government and academia help drive a strong, educated, highly-skilled and talented workforce that meets the needs of employers on day one.

Second, investment in cyber security education has never been higher in Virginia. Leaders from business, government, and education sectors are providing collaborative networks throughout the Commonwealth which create the ecosystem for public-private partnerships to develop. These partnerships often provide the investment and thought leadership in the interest of cultivating and promoting technologies that meet unique cyber security challenges. Recognizing the need for ongoing development, the Commonwealth continues to adopt a "collaborative security model" recommended by leading major internet security firms that promotes shared knowledge while protecting Intellectual Property (IP).[3]

These partnerships are driving innovations in defense and have helped define Virginia as the best place in the nation to do business if you are interested in working with the federal government. Virginia boasts the highest federal defense investment in the nation, and prides itself on such nationally leading programs and institutions as the Going Global Defense Initiative, the Virginia Cyber Security Commission, the MACH37 Cybersecurity Accelerator, the Center for Innovative Technology (CIT), and the Northern Virginia Technology Council (NVTC).

Cyber Security: Protecting Economic Prosperity & National Security

Cyber security is a challenge all Americans face each day whether they know it, or not. From the impact it has on every economic transaction to ensuring the most sensitive databases of personal and private information are secure, cyber protections are considered the most

[1]Sorcher, Sara. The Race to Build the Silicon Valley of Cybersecurity. http://passcode.csmonitor.com/goldrush Accessed June 9, 2016
[2]Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015
[3]http://www.internetsociety.org/globalinternetreport/?gclid=CjwKEAjw4dm6BRCQhtzI6Z6N4i0SJADFPu1ngr-3sRJqBidq2awzkE7SGGgT27n1td2xXR5q4GvwuxoC5hrw_wcB

important enabling technology for the current and future economy. With the expectation that by 2020 there will be 200 billion connected things ranging from cars and planes to cities and animals, the need for securing those connections from external threats has never been more important.[4] In fact, the matter of cyber security threats to American interests has never been more prevalent.

The very way consumers and citizens interact with technology and society has likewise evolved to include significantly greater use of smart phones, tablets, and non-traditional computers, creating vulnerabilities that attackers are already eying. Meanwhile, the threats from abroad come in many forms. Cyber criminals look to attack systems and steal vital information for profit while hackers, hacktivists, and cyber terrorists look to jeopardize vulnerable networks to steal information with mixed motives. Most recently we've seen the direct results of nation-state-funded cyber attacks that are intended to inflict damage politically, economically, and militarily.

The need to maintain a well-protected cyber front is now considered paramount in protecting society as it maintains the validity of vital infrastructure, secures privacy, and ensures economic efficiency while enabling the most basic needs of citizens' access to water, gas, electricity, and financial institutions. Cyber security problems and attacks account for billions of dollars lost each year as devices, accounts, and profiles are sold to the highest bidder, access is lost, or databases compromised.[5] One car hack in 2015 resulted in 1.4 million cars being recalled by Chrysler and the famous hack of Sony resulted in millions of dollars in losses.[6]

As President Barack Obama left office, one of the final policies he and his administration put in place focused on the federal refocusing on cyber security. He declared, "America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property." [7]

As the world's economies become more interconnected, and the way governance is handled relies more and more on the internet and in the Cloud, cyber networks become the backbone of civilization and communication. Unfortunately, with great reliance comes greater vulnerabilities and the same efficiencies that are gained become the weak points in a national security front. In a yearly publication for biggest threats to the country, five of the top six threats were cyber security related with weaponized consumer drones as the only physical threat.[8]

The internet user base has more than tripled since 2005; representing growth from roughly 1 billion users to 3.4 billion users in 2016, while the "touch points" for attack have grown tremendously in the mobile sector.[9] Attacks over the last decade have evolved tremendously and will continue to evolve as internet users grow, avenues of attack are broadened and adversaries adapt, and as governments and private industry become more interconnected. The problem is not going away, and Virginia is leading the charge against these highly adaptive, international foes.

Virginia's Unparalleled Early Recognition of the Importance of Cyber Security

The Commonwealth of Virginia has taken a role of stewardship to both private and public partnerships that enable a collaborative approach to addressing these cyber risks and ranks among the top states in confronting digital threats. Federal and state governments recognized throughout the 1990s and early 2000s that the internet could serve as a catalyst for economic growth, development, and the championing of fast, reliable, and affordable communications—driving job creation, information access, and innovation. It is only more recently that those same policymakers recognized the exposure and costs of less-resilient critical services, disruption of services, e-crime, identity theft, intellectual property theft, fraud, and other malicious cyber activities in terms of economic loss and threat to people's safety and well-being.[10]

The 2014 Deloitte-NASCIO (National Association of State Chief Information Officers) study on cyber security issues found that states have been victims of several high-profile attacks that

[4]https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/2/#4a9c9f3b274c
[5]https://www.mcafee.com/es/resources/reports/rp-economic-impact-cybercrime.pdf
[6]http://www.reuters.com/article/us-sony-cybersecurity-costs-idUSKBN0JN2L020141209
[7]Obama, Barack. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity
[8]https://www.wired.com/2017/01/biggest-security-threats-coming-2017/
[9]http://www.internetlivestats.com/internet-users/#trend
[10]Hathaway et al, "Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index," Potomac Institute for Policy Studies, (forthcoming)

"have resulted in the loss of Personally Identifiable Information (PII) of millions of citizens, including Social Security Numbers, payment card records, dates of birth, driver's license numbers, and tax data." The study recommended "Critical Infrastructure Security and Resilience... should be a shared responsibility between all levels of government and the operators of critical infrastructure."[11] In the 2016 version of the Deloitte-NASCIO survey, researchers found the top issues for states addressing cyber risk were:

- Lack of sufficient funding
- Inadequate availability of cyber security professionals
- Lack of documented processes
- Increasing sophistication of threats
- Lack of visibility and influence within the enterprise[12]

Virginia has addressed these top five issues through enabling legislation, providing specific funding to new programs, cultivating a strong and skilled workforce at the university, community college, and certification levels, and providing much needed guidance and resources to the cyber security industry. This collaborative and cooperative model of shared security and resilience has only been developed and adopted by a few leading states, Virginia among the first.

The cyber security implications for, and impact on, business interests are staggering. In 2016 there was an average of 160 successful cyber attacks per week against businesses in the United States, more than triple the 2010 mark of approximately 50 per week. At the same time, the cost of cyber crime in the United States nearly tripled from $6.5 million in 2010 to $17.4 million in 2016 per company affected, with the largest attack reaping $65 million in damages.[13]

The threat of cyber attacks impacts every nation and every aspect of the world economy, and threats to national security and economic order continue to grow as internet use, interconnected activity, and the development of the Internet of Things (IoT) (the network of physical devices, vehicles, buildings and other items to be sensed and controlled remotely across existing network infrastructure) represent greater "touch points" ready to be accessed for malicious intent. Those touch points represent weaknesses in the cyber armor, and are the very targets of any number of threats. As interconnectedness provides society benefits previously unseen, they also provide hackers, non-state threats, and state-actors an opportunity to access personal information, alter or compromise important databases, and in some cases, even take control of the very vehicle you're riding in. As computing and communications technologies continue to define the next generation of global economy and IoT provides gateways to new data modes, incentives to compromise the security of these systems will likewise grow rapidly.[14]

Why Virginia is the Place to Be for Businesses

Ranked consistently as one of the most pro-business states in the country on the Forbes annual list *Best States for Business*, Virginia offers opportunities for development and expansion of all business interests with a leadership culture that truly understands the importance of maintaining policies that nurtures growth. From tax credits to tax exemptions, performance-based incentives signify Virginia's strong preference for performance-based incentives that reward initiative, investment in local economies, and the building of sustainable infrastructure. The Commonwealth works enthusiastically with new and expanding employers who demonstrate a willingness to invest in those who invest in Virginia, create a high standard of living for Virginians, and enhance local and state economies through increased revenue growth.

Pro-Business Advantages for Companies

- Strategic east coast location and excellent infrastructure provide easy access to national and global markets
- Stable, low tax costs for corporations and individuals and a 6% corporate income tax
- Minimized payroll costs with low worker's compensation rates and a low unemployment tax
- Favorable business environment that protects "at-will" and "right-to-work" employment practices
- One of the highest-ranked states in high-technology employment
- 38 established Technology Zones
- Vibrant and diverse multi-cultural community where employees can live and work
- Experienced, educated and productive workforce
- Recruitment and training programs to help businesses become operational faster and maintain their competitive advantage
- More than 2,300 qualified buildings and sites located across the Commonwealth
- Virginia ranks 3rd in number of Small Business Innovation Research Awards.[15]

[11]Deloitte-NASCIO, "2014 Deloitte-NASCIO Cybersecurity Study"
[12]Deloitte-NASCIO, "2016 Deloitte-NASCIO Cybersecurity Study"
[13]https://www.statista.com/statistics/293274/average-cyber-crime-costs-to-companies-in-selected-countries/
[14]Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015
[15]https://www.nsf.gov/statistics/states/interactive/show.cfm?stateID=53,48&year=0

The Commonwealth of Virginia sees its role in the cyber security ecosystem as one that goes beyond leadership and support to ensure integration of top-level best practices into its infrastructure. After recognizing the need for industry leading cyber security protection, Virginia began adopting industry best practices to lead the nation in protecting their citizens while supporting the innovation environment for growing new companies and new technologies.

In a study by the Pell Center released in November 2015, State of the States on Cybersecurity, Virginia was recognized for its prioritization of the "importance of cyber security, chiefly by prioritizing their state's security and development strategy and through their commitment to increasing their resilience to cyber threats." [16]

The study demonstrated that Virginia is among the leaders in the nation for devising "innovative ways to raise awareness and implement creative solutions to protect state governments and their constituencies... highlight[ing] leading best practices and efforts at the state level to adopt comprehensive cyber security policies and strategies, increasing funding and education, and develop[ing] programs to attract and retain qualified talent.[17]

Virginia was among the first states in the nation to begin adopting National Institute of Standards and Technology (NIST) special publications and benchmarks, such as International Organization for Standardization (ISO 27001 and 27002) and the Control Objectives for Information Technology (CoBIT), to secure data centers and information pipelines.[18] The cyber security mission, enabled by a top pro-business environment, is driving success across industries, through partnerships and relationships with federal and state governments. Virginia's own adoption and inclusion as a state leading the nation furthers the understanding that the Commonwealth is living up to its own high standards for economies. Policymakers in Virginia are leading by example, funding the necessary campaigns to protect and secure government property, systems, and personnel.

Virginia's leadership in the cyber security industry, and its ability to foster new growth in the field, was likely the onus for Governor Terry McAuliffe being named the Chairman of the National Governors Association (NGA). On July 16, 2016, immediately upon his official chairmanship announcement, Governor McAuliffe unveiled his 2016–2017 chair's initiative Meet the Threat: The States Confront the Cyber Challenge, which places states at the center of the finding solutions to the increasingly sophisticated cyber threats facing the nation.[19] Highlighting Virginia's stalwart stance on the issue, Governor McAuliffe illustrated this approach to attendees explaining, "Cyber crime is a growing threat to our states territories, and our nation. As governors, we must be prepared to combat this threat in order to protect the welfare of our citizens...Growing the cyber security industry will create the next generation of American technology jobs and stimulate economic growth in states across the nation." By applying this same approach to the cyber security industry in Virginia, the Governor's office and the rest of the executive leadership team in the Commonwealth look to foster long-term technology growth for the next generation of high-paying jobs and to protect the very infrastructure on which the nation relies.

Virginia Leads the Way

- #1 Best School System in the Mid-Atlantic and Southeast, Wallet Hub (2014)
- #1 Regulatory Environment, Forbes (2015)
- #1 Highest Concentration of Computer Specialists, National Science Foundation (2012)
- #1 State for Higher Education, Smart Asset (2017)
- #2 Highest STEM Job Concentration, Enterprising States Report (2014)
- #2 State with the Highest Concentration of Tech Workers as a Percentage of the Private Sector Workspace, Cyberstates (2015)
- #2 Highest Concentration of Scientists and Engineers, National Science Foundation (2012)
- #2 State or Nation with Most Companies (39) on the Cybersecurity 500 list in the World, Cybersecurity Ventures (2015, Q3)
- #3 Business Friendliness, CNBC (2015)
- #3 Best State for Small Business, Business Insider (2014)
- #5 Top State for Technology and Entrepreneurship, Enterprising States Report (2014)

Photo by Norfolk State University

World Leading Innovation Home to Virginia

Virginia holds the advantage in cyber security just as specialization begins to truly define the next generation of technology economies all over the world. As governments and companies migrate their data to collocated centers hosted and secured by third-party companies specializing in proprietary and confidential data management, a major industry has located and propagated in Virginia. It is estimated, because of this specialization and need for secure data management, that 70% of the world's internet traffic passes through Northern Virginia, largely due to the 68 data centers throughout the Commonwealth.[20]

Virginia is home to many major institutions with extreme data management needs. Recognizing that data management required the very characteristics defining many regions in Virginia, leadership embraced this growing market by passing tax exemptions to companies that buy or lease at least $150 million in computer equipment (between July 2010 and June 2020) for use in data centers. Equinix, one of the earliest data centers founded in Ashburn, Virginia, illustrates why the Commonwealth has become the center for cyber security. In 1998 Equinix chose Ashburn to take advantage of the unique regional characteristics. "Northern Virginia, the patch of American suburbia stretching west and south of Washington, D.C., was home to some of the earliest facilities where carriers interconnected networks and provided access to the internet. The distributed internet exchange, MAE-East, was what brought Equinix to the region, kicking off the development of one of the world's biggest data center markets."[21] Today Equinix operates 10 major data centers in the Northern Virginia regions, in an area in which Facebook leases 40 MW of capacity and Amazon Web Services hosts data alongside DuPont Fabros Technology.

Major investments from Amazon, Microsoft, Bank of America, Northrop Grumman, Google, and others followed for over $9 billion and 7,600 new jobs since 2005 specifically in the development of data centers in Virginia. In 2014 alone, Microsoft announced a plan to expand their $500 million data center by $350 million in Boydton, Virginia offering excellent opportunities to the small town.[22] The growth continues. In 2016, Facebook leased an additional 7.4 MW from DuPont Fabros, Amazon leased 11.3 MW of data from Corporate Office Property Trust, and InfoMart Data entered a deal for a 5.4 MW build-out in a 180,000 square foot building.

The presence and density of these many data centers provide internet traffic security and housing that serve the national capital needs and the federal government. The needs of these unique users foster continued growth and demand in the cyber security space specifically and related technologies more generally. Shared leadership across sectors has created an ecosystem where established enterprises can thrive and new start-ups can innovate to solve newly evolving problems while providing local workforces with high-paying technology focused careers.

The IoT, interconnected devices that transcend computers or mobile phones and are integrated across platforms, represents one of the new challenges

[16]Ibid Pg 4
[17]Ibid Pg 4
[18]Spidalieri, Francseca. State of the States on Cybersecurity. Pell Center for International Relations and Public Policy. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdfNovember 2015
[19]https://www.nga.org/cms/home/news-room/news-releases/2016--news-releases/col2-content/gov-mcauliffe-named-nga-chair.default.html
[20]http://www.nextgov.com/big-data/2016/01/70-percent-global-internet-traffic-goes-through-northern-virginia/124976/
[21]http://www.datacenterknowledge.com/archives/2015/10/15/equinix-doubles-down-in-one-of-internets-most-important-locations/
[22]http://www.datacenterknowledge.com/archives/2014/06/13/microsoft-kicks-350m-data-center-expansion-virginia/

being addressed in the Commonwealth by both established leaders such as GE and start-ups like AconAI. Accelerators and universities are turning out entrepreneurs addressing the next generation of security needs; Virgil Systems and Eunomics of MACH37 exemplify how new and diverse technologies grow in the Virginian economy to meet the demands rising from IoT devices.

Virginia Cyber Security Commission

Through the work of the Virginia Cyber Commission, a holistic, education-centric approach to advancing cyber in the Commonwealth was developed and included in the Governor's introduced budget. Within weeks of coming into office, Governor Terry McAuliffe established the Virginia Cyber Security Commission to both prepare and protect the Commonwealth of Virginia from cyber threats, as well as lay the policy framework that would allow Virginia to provide an excellent regulatory environment for firms working in the cyber security industry.

For Virginia to continue leading in this rapidly evolving space, policymakers and state leaders believe a sustainable talent pipeline capable of providing skilled, industry-ready workers to meet this increasing demand is vital to success. A recent report by the Business Higher Education Forum indicates Virginia has the second highest concentration of cyber job postings behind California. Within the D.C., Maryland, Virginia region, there were over 33,000 cyber security openings—over 17,000 in Virginia alone.[23]

The 2016–2017 Budget Bill includes the following goals proposed by the leadership of Virginia, in collaboration with the Virginia Cyber Security Commission, to continue to meet the needs of industry while ensuring the long-term success of the Commonwealth's energized workforce:

- **Increased number of Cyber Centers of Excellence**
  Provides resources to expand the number of Virginia Community Colleges and Public Universities certified as NSA Centers of Excellence for Cyber Security Education, thereby increasing marketability and opportunity for Virginia students
- **Virginia Scholarship for Service Program**
  Creates a competitive scholarship program to offer tuition relief for up to two years of education in a cyber-related field in return for service as a cyber professional for a Commonwealth Entity. Eligible students will be enrolled in a Virginian Cyber Center of Excellence
- **Veterans Pathway Program in Cyber Security (GMU)**
  Supports student success through expanding a program that allows veterans who complete an Associate's Degree at a Virginia community college to transfer (through guaranteed admissions) to GMU and earn a B.A.S. in Cyber Security
- **Virginia Cyber Range**
  Provides seed-funding for a Commonwealth wide virtual Cyber Range (platform) for students in Virginia high schools, community colleges, and colleges and universities to apply and test their learned abilities. Initial governance for the range will consist of representatives from Virginia's Cyber Centers of Excellence
- **IT Security Service Center (VITA)**
  Supports the cyber security needs of participating Virginia state agencies including, but not limited to, vulnerability scans, information technology security audits, and Information Security Officer (ISO) services
- **Information Sharing and Analysis Organization**
  Establishes Mid-Atlantic Information Sharing and Analysis Organization (ISAO) to provide Virginia with a platform and forum for cross-industry cyber threat information sharing between companies, government (all levels), and universities

[23]https://cyberva.virginia.gov/

- **Virginia Fusion Center**
  Expand cyber capabilities of the Virginia Fusion Center to address cyber threats affecting the safety and security of the public (4 positions)
- **High Tech Crimes Division of Virginia State Police**
  Provides 10 additional positions to High Tech Crimes Division of Virginia State Police to provide investigatory and forensic services to address all types of cyber crime.

The Virginia Cyber Security Commission brought together private and public leaders from throughout the Commonwealth. The commission was co-chaired by Richard Clarke of Good Harbor Security Risk Management and Virginia Secretary of Technology Karen Jackson. While recognized for its overall protection of state government and private enterprise, through the work of the Commission, Virginia invested in several strategic platforms that continue to provide security and resilience to business, education, and governance. There were five subcommittees, each focusing on a specific area of interest to the Commission. These were: Infrastructure (CI), Education and Workforce (ED), Public Awareness (PA), Economic Development (ECON), and Cyber Crime (CC).

These five elements give foundation to the internationally recognized structure for approaching cyber security threats and opportunities. Highlighting these five core elements of cyber security and resilience, the Commonwealth of Virginia Cyber Security Commission pointed to the following achievements in the March 29, 2016 Final Report:

- Became the first state to adopt the NIST Cyber Framework, issued by the President in Executive Order 13636, to provide guidance and a standard for organizations to achieve an effective cyber security posture
- Passed landmark legislation on Digital Identity (SB 814) which now serves as a model for other states and national governments
- Led the nation as the first state to embrace of the Information Sharing and Assessment Organization standard issued by the President in Executive Order 13691
- Clearly established accountability and authority for cyber security in Commonwealth agencies through the passage of new legislation on the role of agency heads (SB 1121)
- Led states in the adoption of the Advanced Credit Card Standard for security (Executive Directive 5)
- Passed four pieces of legislation that improve the ability of the Commonwealth to prosecute cyber crime and develop cyber security policies[24]
- Established the STEM Competition Team Grant Program to promote cyber security focused student development
- Developed a collaborative environment crucial for new cyber security businesses focused on addressing the existing and evolving weaknesses in a broad range of autonomous systems

Though the Commission has been concluded, Virginia leaders and those directly involved in their work, believe a result of that work regarding the development of initial cyber security capabilities for UAV's, automobiles, and advanced manufacturing, is that Virginia is well positioned to generate new cyber industries related to a large portion of the IoT, specifically cyber security for physical systems.[25]

Members of the Commission

Ms. Karen Jackson, *Co-chair, Virginia Secretary of Technology*

Mr. Richard A. Clarke, *Co-chair, Chairman and CEO of Good Harbor Security Risk Management*

Ms. Rhonda Eldridge, *Director of Engineering at Technica Corporation*

Ms. Jennifer Bisceglie, *President and CEO, Interos Solutions, Inc.*

Mr. Paul Kurtz, *Chief Strategy Officer, CyberPoint*

Mr. Paul Tiao, *Attorney and partner with the international law firm of Hunton and Williams, LLP*

Dr. Barry Horowitz, *Munster Professor of Systems and Information Engineering and Chair of the Systems and Information Engineering Department, University of Virginia*

Mr. Andrew H. Turner, *Former Senior Vice President and Head of Global Security, VISA*

Ms. Jandria Alexander, *Principal Director of the Cyber Security Subdivision in the Engineering Technology Group, Aerospace Corp.*

Ms. Elizabeth "Betsy" Hight, *Retired U.S. Navy rear admiral who served as the Vice Director of the Defense Intelligence Agency (DISA)*

Mr. John Wood, *Chief Executive Officer, Chairman of the Board, and Director for Telos Corporation*

Ms. Anne Holton, *Secretary of Education*

Mr. John Harvey, *Secretary of Veterans and Defense Affairs*

Dr. Bill Hazel, *Secretary of Health and Human Resources*

Mr. Maurice Jones, *Secretary of Commerce and Trade*

Mr. Brian Moran, *Secretary of Public Safety and Homeland Security*

[24]Commonwealth of Virginia Cybersecurity Commission. "Threat and Opportunities" August 2015 https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf
[25]https://cyberva.virginia.gov/media/8139/cyber-commission-final-report.pdf

SPOTLIGHT
MACH37 Cyber Accelerator

Nothing exemplifies Virginia's approach to cyber security support greater than the MACH37™ Accelerator—an intensive 90-day program created to launch cyber start-ups—headquartered at Virginia's Center for Innovative Technology (CIT) in Herndon, Virginia. Founded by the CIT and initially funded by the Virginia General Assembly, the Accelerator is designed to facilitate the creation of the next generation of cyber security product companies through mentorship, partnership, and cooperation.

Known as America's premier market-centric cyber security accelerator, the program facilitates the creation of next generation cyber security product companies with emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital.[26] MACH37 has launched 39 innovative cyber security product companies in Virginia since 2013.

MACH37's unique program design places heavy emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital. The accelerator is operated by MACH37 partners, who announced their latest addition, Amazon Web Services, at the highest level of partnership. Other partners include General Dynamics, National Security Services (an SAP company), MITRE, Microsoft BizSpark, Rackspace, Square1bank, and Virtru who all help select which companies are accepted to the program based on their technology, mission, and team.

While promoting robust industry relationships and cross-industry strategies, MACH37 takes cyber security start-up dreams and turns them into realities, driven by free-market economic challenges and helped along by small business support and investment from government. Virginia is leading this wave of innovation by bringing together private industry with government resources, and enabling industry to lead the discussion.

Virginia Cyber Security Partnership

Established in 2012 through a partnership with the FBI, the Virginia Cyber Security Partnership is a collaboration between public and private sectors designed to establish trust for combating cyber threats. The Partnership has more than 220 active members, and has held more than 35 events throughout the Commonwealth.

The mission of the Virginia Cyber Security Partnership (VCSP) is to establish and maintain a trusted community of public and private sector cyber professionals. The Partnership leverages collective experience and knowledge, promotes mutually beneficial information sharing and fosters professional development. This mission seeks to advance the nation's interests.

The VCSP has three primary mission objectives to support short-term and long-term goals.

[26]https://www.mach37.com/explore/cohort-companies/

Skills Enhancement

This mission objective is focused on providing opportunities to sharpen existing skill sets and develop new skills within cyber security. This will be accomplished through workshops, curriculum road maps, etc.

Outreach and Pipeline Development

This mission objective is focused on enhancing the awareness of cyber security and sharing opportunities within the cyber profession to help with enhancing the pipeline of skilled professionals to aid in cyber security. This will also include connecting strong candidates to potential employers.

Collaboration

This mission objective fosters community and strengthens the overall program by creating opportunities for members to collaborate on cyber related activities. This may include networking, outreach, workshops, portal communications, information sharing, etc.

Public Safety

The Virginia Fusion Center

The Virginia Fusion Center (VFC) operates as a focal point within Virginia for the collection, receipt, analysis, and dissemination of timely threat intelligence between the federal government and state, local, and private sector partners.

The VFC strives to operate under an all-hazards approach to threat information, and has developed cyber capabilities utilizing a civilian analyst and sworn special agent detailed from other mission areas to address ongoing cyber activities. These personnel identify and track known and emergent cyber threats to the Commonwealth in support of state-wide awareness, detection, analysis, and response through the dissemination of timely and actionable cyber threat intelligence.

The VFC also provides analytical case support on criminal investigations with a cyber nexus, cyber security training and awareness, and increased cyber resilience through exercise and assessment. In 2014, the VFC produced 43 products related to potential cyber threats and cyber security. In 2016, the Virginia General Assembly funded four additional positions for the VFC.

Virginia State Police High Tech Crime Division

HTCD was formed within the Bureau of Criminal Investigation (BCI) in 2009 by the Department of State Police. The HTCD engages the use of leading technologies to proactively provide specialized law enforcement services in support of the Department's overall mission. In 2016, the Virginia Assembly funded 10 additional positions within the HTCD. Key capabilities include:

- Investigation of "All Forms of High Tech Crimes"
- Investigation of Crimes Against Children
- Computer forensic laboratory services
- On-Scene digital forensic services
- Technical support to federal, state, and local agencies
- Domestic, federal, and international agency liaison

Cyber Guard Prelude

Cyber Guard is a table top exercise that engages state agency partners as well as local, federal, and private sector stakeholders to test state level cyber response procedures. This year's Cyber Guard brought together about 800 participants from 100 organizations. Representatives are here from the Department of Homeland Security, the Defense Department, the FBI, the Federal Aviation Administration and other government agencies, as well as power companies, port facilities, allied foreign partners including Australia, Canada and the United Kingdom, and 10 National Guard teams representing 13 states.

Virginia is training its workforce now.

We provide innovative cyber training to speed worker readiness for the New Virginia Economy:

Cyber Boot Camp: Cyber Education training for high school teachers and students

Conference on Cyber and Education: Discussion and education on the importance of training for cyber careers

Cyber Range: Secure platform built for training, research and collaboration

Virginia National Guard

Building on the efforts and recommendations of the Cyber Security Commission, Virginia is currently partnered with the Virginia National Guard's Data Processing Unit (DPU), capitalizing on the cyber security recommendations to utilize local assets such as the Guard to strengthen the Commonwealth's cyber infrastructure. The partnership conducts cyber assessments on infrastructure within Virginia localities to identify any gaps or opportunities to increase our cyber resilience. Upon completion of the assessment a detailed confidential after-action report is shared with the locality. As of July 2016, three missions have been completed, with an additional six identified in the near-term. Virginia's proactive stance in addressing cyber security has also led the Air National Guard to select Virginia as a location for their cyber guard unit.

Virginia's Commitment to Cyber Security in Higher Education

In 2016, the Commonwealth instituted two grant programs that support students seeking education and credentials in cyber security related fields. These grants bolster the current commitment to STEM fields provided by the Two Year College Transfer Grant Program.

Cyber Security Scholarship

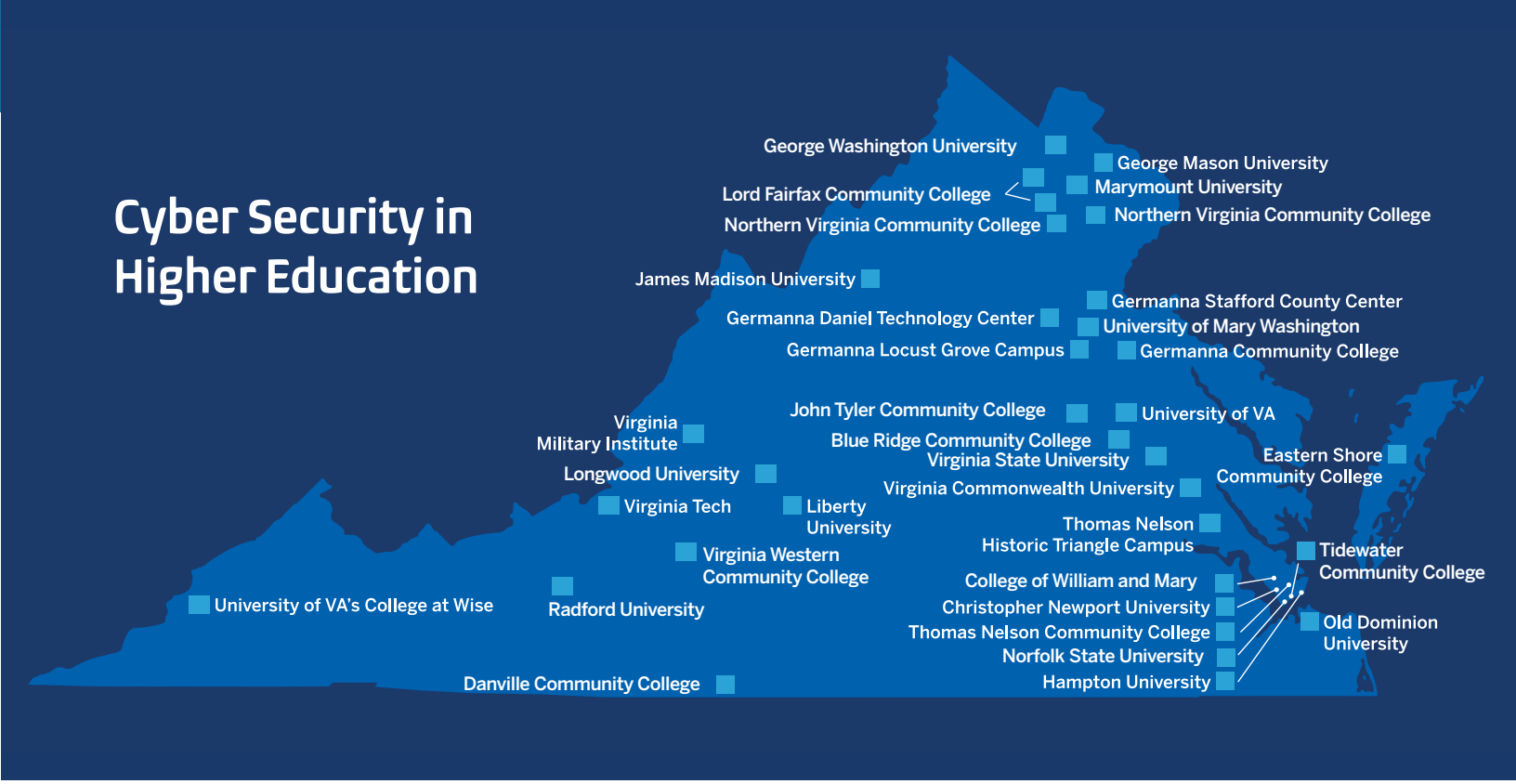
Offered through the State Council on Higher Education in Virginia, the Cyber Security Scholarship is designed to obtain commitments from students to work in state government in the field of cyber security. $500,000 has been appropriated for this program in the 2016-2017 Academic Year.

New Economy Workforce Credential Grant Fund and Program

This grant opportunity supports students as they complete high demand workforce credentials. While a list of eligible programs in currently being developed by the State Workforce Board, information technology and cyber security are both in high demand and currently emphasized.

Two-Year College Transfer Grant Program (CTG)

CTG qualifying students receive $1,000 per year if enrolled in STEM programs, such as information technology or cyber security degree programs.



Workforce and Education

Technology companies are supported in Virginia by infrastructure that outperforms other states, and a pro-business environment geared toward innovation and IP protection that have been made even stronger with recent legislation. They are also supported by a robust, educated, and well-developed workforce and a world-leading university system that produces thousands of graduates in cyber-related fields annually and have direct and immediate impacts on national security. Supporting these industries are continued national and state funding announcements and allocations that recognize Virginia's leadership.

On August 2016, Senator Mark Warner and Senator Tim Kaine announced a nearly $20 million grant from the National Science Foundation (NSF) to "...help increase cyber workforce development and encourage scientific partnerships to deliver innovation in the field." As Senator Warner says, "This award will help Virginia Tech—one of the top research institutions in the country—to attract the best and brightest young minds into careers in computational molecular science and cyber technology, and allow Virginia to continue to establish a leadership role in the cyber field."[27]

Other Commonwealth cyber security highlights from the past year include:

- **The New Economy Workforce Credential** initiative signed into law a statewide program to allow Virginia residents to obtain non-credit workforce training at 1/3 of the cost, at any community college or participating regional higher education center, for college-approved industry-recognized certifications aligned with high demand occupations. The initiative provides financial aid for non-credit workforce training.
- **US Chamber of Commerce Foundation's Talent Pipeline Management** initiative sought to build talent pipelines and provide high quality job opportunities in the occupations of Computer Programmer/Software Developer and Cyber/Information Security Engineer/Analyst.
- Virginia has officially launched a cyber security apprenticeship program. Businesses and state agencies sponsoring new registered apprentices in IT or cyber security occupations are now eligible for up to $1,000 annually, per apprentice, in state fiscal support.
- **The Virginia Community College System** will soon launch a veterans' portal showing how college credit is awarded for military experience. With over 800,000 veterans in Virginia, connecting military education and training in IT and cyber security to postsecondary education credentials is important to ensuring the Commonwealth's cyber security workforce.

[27]https://homelandprepnews.com/government/19417-virginia-tech-awarded-20-million-grant-cyber-workforce-development/

- **Norfolk State University** leads a $25 million collaborative effort funded by the Department of Energy (DOE) to develop a K-20 pipeline for the cyber security workforce.
- **The Military Occupational Specialty (MOS) to Degree Program** at NOVA Community College and the **Veterans Pathway Program in Cyber Security** at George Mason University create a seamless pathway for veterans to use military experience toward the completion of an Associate's Degree and earn a B.A.S in cyber security.
- **Virtual Cyber Range**. The Governor's biennial budget included $4 million for the creation of a Commonwealth-wide virtual cyber range housed at Virginia Tech that will allow our next generation of cyber professionals to sharpen their skills for detecting and preventing attacks.

Workforce

Maintaining a highly skilled workforce is a fundamental component to ensuring future success. As Virginia has led the nation in the adoption of vital protections for infrastructure and data security—creating one of the most vibrant, protected, and diverse technology ecosystems in the world—it has also been focusing on creating a specialized workforce through its nationally ranked public and private education system through funding, investments, and public-private partnerships.

Virginia currently has over 67,850 people working in cyber security, and many of Virginia's universities are at the forefront of cyber security research and development. Per the Bureau of Labor Statistics, Virginia ranks first in the nation in the percentage of computer systems analysts and computer software. Virginia also ranks second in concentration of its workers in the tech industry and leads the nation with a ratio of 25 job postings per 10,000 residents by state.[28] Virginia's population of over 8.3 million and a workforce of more than 4.2 million boasts the 6th highest education rate in the nation for those with a minimum of a bachelor's degree at 36.9%. Additionally, roughly 18,000 people leave Virginia military bases seeking civilian employment annually; these are highly skilled, trained, educated, and hard working workforce entrants often with increased security clearances and national security interests.

- Virginia currently supports the 3rd highest concentration of technology jobs as a share of overall private-sector employment.
- More than 1,400 doctorate degrees in science and engineering are awarded annually from Virginia universities
- More than 15,000 science and engineering graduate students pursue advanced degrees in Virginia
- Virginia ranks 8th in the nation for the number of employed workers with doctorate degrees
- Approximately 18,000 people leave Virginia military bases each year and enter the civilian workforce

This workforce includes the high-tech skills found in our northern Virginia Technology Corridor, highly skilled veterans returning to civilian life from one of the many regional defense installations, and leading edge research performed at our universities and local federal laboratories which then transfers easily to business success at all levels of an organization.

Veterans

Currently, around 800,000 veterans live in Virginia, and that number grows by 2,000 a year. With a strong military presence, defense activities and civilian contractors, Virginia is a natural leader in veterans affairs and trailblazer in developing veteran employment strategies. Through experience and training, veterans retain the kind of technical talent needed to help build the workforce of the 21st century.

Cyber Security Apprenticeship Program

Since June of 2016, businesses have the opportunity to stand up registered apprenticeships for cyber security occupations. Formally approved by the Virginia Apprenticeship Council, the three new registered apprenticeship cyber security occupations include: Information Security Analyst - Cyber Security Analyst, Information Security Analyst - Computer Forensics Analyst, and Information Security Analyst - Incident Response Analyst. In September

[28] http://passcode.csmonitor.com/goldrush

Photo by Virginia Cyber Range

of 2016, the Commonwealth celebrated the establishment of Virginia's first registered cyber security apprenticeship, a partnership between Tidewater Community College (TCC) and Yorktown-based Peregrine Technical Solutions, LLC.

Introducing registered apprenticeship occupations in an industry sector like cyber security that has not traditionally employed apprentices will boost the ability of young adults and career switchers to attain in-demand skills and even earn industry certifications and college credits. These programs bolster Virginia's national leadership in cyber education and training and commitment to preparing our students for the jobs of the future. These apprenticeships lay a firm foundation for this emerging sector.

Education

The Commonwealth's commitment to integrating cyber security into education pathways has already begun. The Cyber Security Commission hosted the Commonwealth Conference on Cyber and Education on December 2, 2015, to refocus and engage educators, employers, and government on the immediate and future needs and opportunities defined by the cyber security challenge. As one result, the Virginia Department of Education established Cyber Security as a career pathway that begins with career and technical education programs in middle grades and high schools. This includes the creation of Virginia's Cyber Security and Cyber Forensics Infusion Units, which have identified 85 tasks/competencies that can be incorporated into existing technology or STEM courses.

- Basic Operations and Concepts
- Social and Ethical Issues
- Technology Research Tools
- Thinking Skills
- Problem Solving and Decision-Making
- Technology Communication Tools
- Leadership Development Expectations

The Governor also established two STEM Academies (Marshall and Chantilly) focusing on cyber security during summer months; supplementing the 20 other STEM focused academies in Virginia.[29] The Virginia General Assembly allocated grant funds for 32 cyber camps in the summer of 2016 through the Virginia Department of Education. Seventeen of Virginia's 23 community colleges offer one or more courses aligned to cyber security, and eight offer security certificates. Three—Lord Fairfax Community College, Northern Virginia Community College, and Tidewater Community College—are designated as National Centers of Academic Excellence, with more pursuing accreditation. With the growth of new programs around the Commonwealth, the Virginia Community College System saw huge enrollments in the 2015–2016 scholastic year at 111,124 full-time students and 252,758 total student enrollees (including those who attend for certifications or specific accreditation).[30]

[29]http://www.doe.virginia.gov/instruction/career_technical/gov_academies/
[30]http://www.vccs.edu/about/where-we-are/impact/

SPOTLIGHT
The Virginia Cyber Range

The Virginia Cyber Range (VCR) is the next step in creating the top educational system in the world for addressing cyber security challenges through partnership, collaboration, and the leveraging of the area's unique assets and resources. The VCR provides an extensive courseware repository for educators and a cloud-hosted environment for hands-on cyber security labs exercises for students. The VCR is the reimaging of education and an exercise in addressing threats in the domain in which it exists—online, cloud-based, and future focused. The VCR was proposed by Governor McAuliffe in Spring 2016 as part of his vision to boost Virginia's cyber security industry through strategic educational investments. The executive committee leading the range represents public institutions that are nationally recognized centers of academic excellence in cyber security within the Commonwealth and are therefore uniquely positioned to create the best curriculum for the initiative.

The Virginia Cyber Range consists of the following three core concepts that enable student development in cyber security skills:

- **Labs and Exercises**
  The primary feature of the Virginia Cyber Range is a cloud-hosted, virtual environment where students will practice what they have learned in immersive, hands-on laboratory exercises to complement their cyber security courses. Large-scale exercises and extensive "capture-the-flag" exercises will soon be offered in Summer 2017.
- **Courseware Repository**
  The Virginia Cyber Range will contain a repository of cyber security courseware to support full high school and college courses on various cyber security topics such as secure network configuration and network defense, digital forensics, penetration testing, cyber law and policy, and other topics. Course material will be offered in modular form to allow flexible adoption of offerings and customization of courses to meet individual institutional and faculty needs. Accessible only by faculty members at Virginia public high schools and colleges, the repository will be indexed and searchable and will contain course content such as syllabi, lesson plans, presentation slides, and representative homework exercises and exams.
- **Community of Purpose**
  The third core element, and vital to the success of students and faculty working in an online environment, is building a community across educational institutions with which to ask questions, connect offline, and develop strong ties. The Virginia Cyber Range will convene workshops to "teach the teachers" and improve cyber security education at consortium institutions and to develop a shared understanding of future needs for cyber security education and gaps.

Currently, the Cyber Range is supporting hands-on exercises and educational content for over 250 students in three courses at two different Virginia colleges. Additional courses are in development and more courses across the Commonwealth will use the Cyber Range during fall 2017. The initial focus of the Virginia Cyber Range is to serve Virginia colleges and universities, but will expand to serve high school students, starting with support for student and teacher cyber security camps this summer.

The VCR provides a new mechanism for state governments to provide efficient, effective, and meaningful partnership between major institutions. By providing a fully immersive, but fully online educational environment, the Commonwealth is pushing the limits on traditional education and thereby bringing the next generation of students into a much-needed workforce. This workforce will be skilled in topics such as Secure Network Configuration, Network Defense, Reverse Engineering, Cryptography, Incident Response, Penetration Testing, Security Data Analytics, SCADA and Industrial Control Systems, Cyber Law, and Cyber Policy. By supporting all students with this collaborative, not just those attending the various specialized cyber security institutions in Virginia, all students gain access to training. This innovative educational model may even be the future of specialized education.

Virginia Cyber Cup

Hosted by the Virginia Cyber Range, the Virginia Cyber Cup is a "capture the flag" competition in which competing university teams tackle problems in scenarios designed to model real-world computer security challenges across a range of categories including cryptography, network traffic analysis, reverse engineering, steganography, and more. An understanding of historical and modern security vulnerabilities was helpful to gain the most of this experience. With challenges ranging from introductory to advanced, this annual competition is designed to both test skills and teach concepts.

Amazon Web Services

As an example of Virginia's many public-private partnerships, the new strategic relationship between Amazon Web Services (AWS) and the Virginia Cyber Range expands the reach of the initiative and helps make Virginia a national

resource for cyber security education. AWS will join the Commonwealth of Virginia and Virginia Tech to support scalable cloud infrastructure and collaborate on cyber security educational efforts, enabling the Cyber Range with both content and a closed network for hands-on exercises, competitions, and other simulations.

Cyber Security Centers of Excellence

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA/CD programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. This unique designation is valid for five academic years, after which the school must successfully reapply to retain its CAE designation.

Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. CAE IA/CD institutions receive formal recognition from the government as well as opportunities for prestige and publicity for their role in securing our nation's information systems.

National Centers of Academic Excellence in Virginia[31]

College/University	Programs offered		Honors
George Mason University Fairfax, VA 4 Year Public	Masters Degree	M.S. in Information Security and Assurance	
		M.S. in Applied Information Technology with concentration in Cyber Security	
		M.S. in Computer Forensics	
		M.S. in Data Analytics with concentration in Digital Forensics	
		M.S. in Management of Secure Information Systems	
	Bachelors Degree	B.S. in Information Technology with concentration in Information Security	
		Bachelor of Applied Science with Concentration in Cyber Security	
		B.S. in Cyber Security Engineering	
	Graduate Certificate	Graduate Certificate in Applied Cyber Security	
		Graduate Certificate in Information Security and Assurance	
		Graduate Certificate in Tactical Computer Operations	
		Graduate Certificate in Telecommunications Forensics and Security	
	Center/ Institute	Mason Center for Security Information Systems	
		Center for Assured Research and Engineering	
George Washington University Washington, D.C. 4 Year Public	Certificate	Certificate in Computer Security and Information Assistance	National Center of Excellence in Information Assurance Education National Center of Excellence in Information Assurance Cyber Defense Research
	Center/ Institute	Cyber Security Policy and Research Institute	
Hampton University Hampton, VA 4 Year Private	Masters Degree	M.S. for Information Assurance	Center of Academic Excellence in Information Assurance Education NSF CyberCorps Scholarship for Information Assurance recipient
James Madison University Harrisonburg, VA 4 Year Public	Masters Degree	M.S. in Computer Science with concentration in Information Security and Digital Forensics	National Center of Excellence in Information Assurance Education NSF CyberCorps Scholarship for Information Assurance recipient
		M.B.A. with concentration in Information Security	
	Bachelors Degree	B.S. in Intelligence Analysis	
	Certificate	Certificate in Information Systems Security	
		Certificate in Network/Information Security	
	Professional Development	VATCyber Boot Camp and GenCyber Boot Camp instructing teachers in cyber security education	

[31]https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

College/University	Programs offered		Honors
Longwood University Farmville, VA 4 Year Public	Minor	Minor in Cyber Security, Forensics and Policy	National Center for Digital Forensics Academic Excellence by U.S. Department of Defense
	Partnerships/ Consortiums	Partners with Commonwealth Center for Advanced Logistics Systems	
Lord Fairfax Community College Middletown, VA 2 Year Public	Career Studies Certificate	Career Studies Certificate in Cyber Security	National Center of Academic Excellence in Cyber Defense for 2 Year Education
	Associates Degree	A.A.S. in Information Systems Technology with concentration in Cybersecurity	
Marymount University Arlington, VA 4 Year Private	Masters Degree	M.S. in Cybersecurity	Center for Academic Excellence in Cyber Defense NSF CyberCorps Scholarship for Information Assurance recipient
		M.S. in Information Technology with concentration in Cybersecurity	
		Dual Degree Program (M.S. in Information Technology and M.S. in Cybersecurity)	
	Bachelors Degree	B.S. in Information Technology with concentration in Networking and Cybersecurity	
	Combined Degree Program	Combined B.S./M.S. Program in Information Technology and Cybersecurity	
	Graduate Certificate	Graduate Certificate in Cybersecurity	
	Certificate	Undergraduate Certificate in Computer Networking and Cybersecurity	
Norfolk State University Norfolk, VA 4 Year	Masters Degree	M.S. in Computer Science with concentration in Information Assurance	Center of Excellence in Cybersecurity Research Center of Academic Excellence in Cyber Defense Education Consortium Enabling Cybersecurity Opportunities and Research Grant recipient
		M.S. in Cyber Security	
	Bachelors Degree	B.S. in Computer Science with concentration in Information Assurance	
Northern Virginia Community College Annandale, VA 2 Year Public	Associates Degree	A.A.S. in Cybersecurity	National Center of Academic Excellence in Information Assurance for 2 Year Education

College/University	Programs offered		Honors
Radford University Radford, VA 4 Year Public	Masters Degree	M.S. in Data and Information Management with course in Security Analytics	Center for Academic Excellence in Cyber Defense
	Bachelors Degree	B.S. in Computer Science and Technology with course in core security	
		B.S. in Information Science and Systems with course in core security	
	Certificate	Certificate in Information Security	
	Course	Graduate course in cyber security education for K-12 teachers	
Tidewater Community College Norfolk, VA 2 Year Public	Associates Degree	A.A.S. in Information Systems Technology with an emphasis in Cybersecurity	National Center of Academic Excellence in Information Assurance for 2 Year Education
	Career Studies Certificate	Career Studies Certificate in Cybersecurity	
Virginia Tech Blacksburg, VA 4 Year Public	Minor	Minor in Cybersecurity	Intelligence Community Center for Academic Excellence NSA/DHS Center for Academic Excellence NSF CyberCorps Scholarship for Information Assurance recipient
	Graduate Certificate	Graduate Certificate in Cyber Security	
	Laboratory	Information Technology Security Laboratory	
	Center/ Institute	Security and Software Engineering Research Center	

National Initiative for Cybersecurity Education

The National Initiative for Cybersecurity Education (NICE) is a nationally coordinated effort to advance education and training opportunities for cyber security career preparation. NICE is coordinated by the National Institute of Standards and Technology, an agency of the Department of Commerce.

NICE defines the work within the cyber security field to help maintain a globally competitive cyber security workforce and broaden the pool of skilled workers capable of supporting a cyber-secure nation. It includes federal departments and agencies, industries, and academic institutions beginning with K-12.

NICE has 13 Virginia affiliates, including seven educational institutions: George Mason University, Hampton University, James Madison University, Marymount University, Norfolk State University, Northern Virginia Community College, and Virginia Tech. Virginia boasts 12 universities with the Center of Academic Excellence designation and 18 Virginia universities currently offer cyber security related degree programs.

As Virginian universities have contributed to preparing the workforce by offering various degrees associated with cyber security/information technology, they also support activities to enhance traditional course offerings with competitions, challenges, and student scholarship programs. The following are some examples of the cyber security focused challenges, competitions, and successes from around the Commonwealth:

- **George Mason University's** Volgenau School of Engineering became the first college in the nation to offer a cyber security engineering degree that focuses on cyber-resilience engineering design in Fall 2015. It also runs summer camps for children and outreaches to high school students, boosting interest in the STEM fields.
- **George Mason University** has joined a new research and training initiative of the U.S. Army Reserve (USAR), the Cyber P3, which is a public-private partnership designed to enhance operational readiness in the Army. The initiative also seeks to address the national shortage of cyber security professionals. Mason's #7 ranking by Ponemon Institute and HP as a top national cyber program was an important factor used by USAR to select the initial group of six universities with which to launch the partnership.
- **Norfolk State** leads a $25 million effort that begins with kindergarten activities to develop cyber security professionals. Funded by the Department of Energy, Norfolk State is leading a consortium of Historically Black Colleges and Universities, a school division, and the Department of Energy National Laboratories to develop STEM education that will lead to security careers.
- **Virginia Tech, James Madison University, Marymount University, and Hampton University** participate in the Federal CyberCorps Scholarship for Service program, which provides full tuition and up to $25,000 per year in scholarships to students interested in pursuing careers in cyber security. The program is open to students majoring in computer science or computer engineering.[32]
- **James Madison University** hosts a cyber security boot camp, called GenCyber, for high school teachers and K-12 students. The program provides cyber security awareness and education to students, cyber security teaching methodologies for computer science teachers, and establishes resources for both cyber security teaching and learning curricula during the summer each year to raise awareness and encourage the integration of cyber security topics into the curriculum.[33]
- **Virginia Tech** hosted the 2015 U.S. Cyber Challenge and Cybersecurity Camp for high school students in the eastern United States. This competition sought to recruit 10,000 of America's brightest students to usher into next generation cyber security professional jobs.
- **Virginia Tech** is leading the creation of the Virginia Cyber Range which brings together faculty from George Mason University, James Madison University, Longwood University, Norfolk State University, Virginia Tech, and Radford University, as well as faculty from Lord Fairfax Community College, Northern Virginia Community College, and Tidewater Community College (all Centers of Academic Excellence in Cybersecurity or Digital Forensics) to create a mostly online cyber security training platform.

A University of Virginia student and faculty team competed in the National Cybersecurity Challenge in August 2016, taking home the second-place prize of $1 million dollars. This team, a collaboration between GrammaTech and UVA faculty and students, went head to head with the championship team and was recognized for discovering security threats that had been unrecognized even by the DARPA team running the competition.

[32]http://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education
[33]https://www.jmu.edu/cs/community-involvement/gencyber/index.shtml

Virginia's Cyber Security Industry

Success in developing an industry can be seen in how the companies, workforce, and products are received in the market place, and in all three indicators Virginia is leading the nation. Thirty-one of the top 100 Federal Contractors per Washington Technology Top 100 are headquartered in Northern Virginia's Fairfax County, with 82 of them having operations there. In the past five years, there have been over 20 announcements related to cyber security plans to create an additional 980 jobs from companies such as Cyber Defense Solutions, FoxGuard Solutions, Telos, Kaspersky Government Security Solutions, Technology Management Solutions, and GE.[34] Demand is expected to continue to grow in this technology sector through at least 2020 with the number of persons employed in this occupational group in the Commonwealth expected to increase by 25% through 2022, surpassing the national expectation of just over 17% in that same timeframe.[35]

Companies Listed in the Top 500 Cybersecurity Companies in the World located in Virginia

Company	Cybersecurity Sector	Corporate HQ
Sera-Brynn	Cyber Risk Management	Suffolk, VA
IKANOW	Information Security Analytics	Reston, VA
VeriSign	Internet Security Solutions	Reston, VA
Northrop Grumman	Cyber & Homeland Security Services	McLean, VA
L-3	National Security Solutions	Reston, VA
Novetta	Cyber Security Analytics	McLean, VA
Leidos	Anti-Terrorism & Homeland Security	Reston, VA
CYREN	Web, Email & Mobile Security	McLean, VA
CyFIR	Digital Forensics & e-Discovery	Manassas, VA
Haystax	Advanced Threat Analytics	McLean, VA
LookingGlass	Cyber Threat Intelligence Management	Arlington, VA
SAIC	Cybersecurity Professional Services	McLean, VA
Siemens Government Technologies	Cybersecurity for Federal Government	Arlington, VA
ThreatQuotient	Threat Intelligence Platform	Reston, VA
MeasuredRisk	Cyber Advisory & Risk Analysis	Arlington, VA
Centripetal	Cyber Threat Intelligence	Herndon, VA
Paraben	Digital Forensics & Data Recovery	Ashburn, VA
MindPoint Group	IT Security Solutions	Springfield, VA
Ntrepid	Secure Network & Online Computing	Herndon, VA
Oberthur Technologies	Digital Security for Mobility	Chantilly, VA
CACI	Intelligence, Defense & Federal Security	Ballston, VA
General Dynamics	IT Cybersecurity Solutions	Fairfax, VA
PhishMe	Phishing Attack Defense	Leesburg, VA
MicroStrategy	Mobile Identity Platform	Tysons Corner, VA

[34]http://www.yesvirginia.org/Content/pdf/Industry%20Profiles/VA%20Cybersecurity%20Summary%202016.pdf
[35]Idib Pg 4

Company	Cybersecurity Sector	Corporate HQ
Daon	Identity Assurance & Biometrics	Fairfax, VA
PFP Cybersecurity	IoT Security	Vienna, VA
Defense Point Security	Cybersecurity Services for Federal Agencies	Alexandria, VA
CSC	IT Security Services	Falls Church, VA
Invincea	Malware Detection & Prevention	Fairfax, VA
Endgame	Security Intelligence & Analytics	Arlington, VA
ePlus Security	Infosecurity Services & Products	Herndon, VA
Verodin	Cyber Attack Simulations	Reston, VA
AxonAI	Internet of Things Security	Harrisonburg, VA
Cigital	Application Security Testing	Dulles, VA
ThreatConnect	Cyber Threat Intelligence Platform	Arlington, VA
GuidePoint Security	Information Security Services	Reston, VA
Risk Based Security	Cyber Risk Analytics	Richmond, VA
SurfWatch Labs	Cyber Risk Intelligence Analytics	Sterling, VA
Distil Networks	Malicious Bot Detection & Prevention	Arlington, VA
Veris Group	Cybersecurity Professional Services	Vienna, VA

Virginia is also the headquarters to several IT Security Consulting companies such as Booz Allen Hamilton, who are all expecting to see a 68% rise in revenues industry wide. Industry partners in the public and private sector are among Virginia's greatest assets in developing the strongest cyber security portfolio internationally. To meet the increased demand for cyber security, IT, and systems infrastructure specialists, Virginia's universities have established over one dozen degree and certification programs in Computer and Information Systems Security/Information Assurance.

Success Stories

Sera-Brynn[36]

Sera-Brynn, headquartered in Suffolk, Virginia and opened a second office in Northern Virginia, increased its elite standing atop the cyber security firms by moving up to number seven in the United States and continuing at number ten in the world rankings of like companies.[37] Sera-Brynn approaches the cyber security partnerships collaboratively as illustrated by CEO Rob Hegedus who said, "Addressing cyber security requirements and response activities is more and more becoming a community-based approached." Sera-Brynn's clients include Fortune 1000 companies, healthcare, financial institutions, insurance carriers and reinsurers, higher education, municipalities and state governments, manufacturers, law offices, and more.

Leidos[38]

Leidos, headquartered in Reston, Virginia, and boasting $10 billion in annual revenue, exhibits core competencies in C4ISR, Cyber, Systems Engineering, Large-Scale Agile Software Development, Data Analytics, Enterprise IT Modernization, and Operations & Sustainment all relating to Department of Homeland Security, Department of Defense, as well as Intelligence, Civil, and Health System domains. Leidos recently ranked 81st on the top 500 cyber security companies in the world.

Invincea[39]

With technology born out of a joint program between company founders and George Mason University's Center for Secure Information Systems, Invincea has become a leader in the protection of IT threats that impact business. More than 25,000 customers now rely on Invincea to prevent and detect threats and to enable their workforce in diverse climates. Invincea is now ranked 123rd on the top 500 Cybersecurity firms in the world.

[36]https://sera-brynn.com/sera-brynn-moves-top-10-u-s-cybersecurity-500-top-global-cybersecurity-firms/
[37]https://sera-brynn.com/sera-brynn-recognized-for-its-expansion-and-innovative-service-offerings-on-the-cybersecurity-500-list/
[38]https://www.leidos.com/
[39]https://www.invincea.com/

PhishME[40]

PhishME, headquartered in Leesburg, Virginia, recently ranked 93rd on the top 500 Cybersecurity companies in the world. By targeting phishing attacks, still one of the largest cyber security threats facing consumers, PhishME attempts to target the biggest problems first. 91% of all breaches start with spear phishing with an average time of 146 days before identifying the breach and $4 million the average cost of such a breach.[41] Incorporated in 2011, PhishMe is the leading provider of phishing threat management for organizations concerned about human susceptibility and response to advanced targeted attacks. PhishMe's intelligence-driven solutions empower employees to be an active line of defense and source of attack intelligence by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats.

CYREN[42]

CYREN, ranked 95th on the World Cybersecurity Top 500, and headquartered in McLean, Virginia, is a global leader in information security solutions for protecting web, email, and mobile transactions. They continuously innovate through cloud-based threat detection and proactive data analytics to provide security solutions to businesses of all sizes. Their patented technologies increase the value and profitability of their partners' solutions—protecting over 550 million end users worldwide.

L-3 & Northrop Grumman

L-3 Communications and Northrop Grumman offer a diverse, compelling platform of cyber security products and platforms and are both based in Virginia (Reston and McLean respectively). Ranked 55 and 46 in the top cyber security firms in the world, federal, state, and private entities can incorporate world leading technologies easily.

Federally Funded Research Centers in Virginia

Facility	Location
National Security Engineering Center	Bedford, MA McLean, VA
Center for Advanced Aviation System Development	McLean, VA
Center for Enterprise Modernization	McLean, VA
National Security Engineering Center	Bedford, MA McLean, VA
Center for Advanced Aviation System Development	McLean, VA
Center for Enterprise Modernization	McLean, VA
Centers for Communications and Computing	Alexandria, VA
CMS Alliance to Modernize Healthcare	McLean, VA
Homeland Security Studies and Analysis Institute	Arlington, VA
Homeland Security Systems Engineering and Development Institute	McLean, VA
Judiciary Engineering and Modernization Center	McLean, VA
National Radio Astronomy Observatory	Charlottesville, VA
Studies and Analyses Center	Alexandria, VA
Thomas Jefferson National Accelerator Facility	Newport News, VA

Federal Entity Offices in Virginia

Facility	Location
Langley Research Center (LaRC)	Hampton, VA
Wallops Flight Facility	Wallops Island, VA
Thomas Jefferson National Accelerator	Newport News, VA
United States Patent and Trademark Office (PTO)	Alexandria, VA
National Cybersecurity & Communications Integration Center	Arlington, VA
Air Force Office of Scientific Research (AFOSR)	Arlington, VA
National Science Foundation (NSF)	Arlington, VA
Office of Naval Research (ONR)	Arlington, VA
United States Fish & Wildlife Service	Falls Church, VA
Foreign Service Institute	Arlington, VA
Nuclear Waste Technical Review Board	Arlington, VA
US Marshals Service	Arlington, VA
Army National Guard Readiness Center	Arlington, VA
Joint Improvised Explosive Device Defeat Organization	Arlington , VA
United States Air Force (USAF)	Arlington , VA

[40]https://phishme.com/
[41]https://phishme.com/product-services/pm-solution/
[42]http://www.cyren.com/

The Federal Connection: Cyber Security Investments & Initiatives

Proximity to Decision-makers

Virginia exhibits unique qualities that no other state in the nation can claim, and truly no other region in the world can provide. Its location provides direct engagement and access to the nation's political decision-making center in Washington, D.C. With unparalleled access to federal legislators and the executive branch, educational and business groups have seen it in their own best interests to call Virginia home. With the federal cyber security market estimated to grow from $18 billion in 2017 to $22 billion by 2022 with a 4.4% Compound Annual Growth Rate (CAGR), proximity to Washington, D.C. has never been more important for firms.[43]

Virginia is home to several federal agencies that focus on cyber security and offer contract relationships to the industry including the Army Cyber Command (ARCYBER), Department of Defense, Department of Homeland Security's National Cyber Security and Communications Integration Center, and the Defense Advanced Research Projects Agency (DARPA).[44] Educational partners such as the International Cyber Center (ICC) at George Mason University, The Center for Secure Information Systems (CSIS), Cyber@VT and the Hume Center for National Security and Technology, The Cybersecurity Innovations Laboratory, and James Madison University's Institute for Infrastructure and Information Assurance (IIIA) interface directly with these agencies, providing mechanisms and opportunities for professionals, educators, and students to engage with federal agencies and private companies like L-3 Communications and Amazon Web Services.

Engagement across industries, governments, and markets is the fundamental key to the Commonwealth's leadership success and provides a unique framework for success recognized as a national leader. When coupled by the Commonwealth's extensive business incentives programs and state leaders who understand the importance of cyber security investment, no other state can compete.

NASA & the Defense Industry

The National Aeronautics and Space Administration (NASA) and the defense industry should not be overlooked as unique partners for opportunity in Virginia. While the defense industry is spread throughout the nation, Virginia's position is unique in the breadth of contracts and relationships available through the Department of Defense (DoD).

As of FY 2015, Virginia accounted for more than $40.3 billion in defense prime contracts alone, making it the number one state for total revenue driven by DoD investment.[45] This success is not driven simply by the geographical access to Washington D.C., but by the long-term investments made by leading companies and government agencies in the region, an investment that is likely to continue growing with the business friendly environment and partnership development in cyber security as well as a renewed focus on defense and security spending in Washington, D.C.

Twelve of the top defense contractors are headquartered in Virginia, including Alliant Techsystems, Atlantic Diving Supply, Booz Allen Hamilton, CACI, CSC, DynCorp, General Dynamics, Huntington Ingalls, ITT Exelis, Leidos, ManTech, and Northrop Grumman. While such heavy-hitters in the same field may intimidate some companies, by being co-located in the Virginia area, new companies gain access to corporate entrepreneurial initiatives that enable cross-collaboration, increased likelihood of buyout, and a "Silicon Valley" like atmosphere focused in their field.

These defense contractors have seen the value in access to national leaders in Washington D.C., as well as a proximity to the Pentagon and 19 defense installations. With the federal government focusing on investing in start-up companies by making access to venture capital easier for government related tech firms, localizing a business in Virginia has never been more important.[46]

These 19 defense installations have cultivated programs that enable service members and procurement officers to engage with communities in the industry. By collaborating locally, diminishing the need for travel expense and increasing face-to-face communication and discussion, cyber security companies gain a leg up on any non-local competition. Defense installations, defense contractors, and smaller firms create collaborative partnerships and projects much more easily than with other organizations, leading directly to research and development capabilities throughout the state.

Research and development is the first fundamental step toward innovation. By collaborating with competitors and developing private-partnerships that enable potential customers to outline

[43]https://www.marketresearchmedia.com/?p=206
[44]Idib Pg 6
[45]http://www.yesvirginia.org/KeyIndustries/Aerospace
[46]https://www.whitehouse.gov/startup-america-fact-sheet

their needs directly to engineering production, the interactive process of innovation comes faster and with much greater return. Virginia has therefore made these partnerships its focus over the last five years, and the area is reaping the rewards of those efforts.

Virginia now boasts significant partnerships between NASA, DoD, and private companies. The Virginia Modeling and Simulation Center (VMASC) applies simulation techniques to solve problems and provides training for industry, military, and governments. Virginia's unique partnerships also include the Defense Advanced Research Projects Agency (DARPA) that enables private companies and universities to respond to military proposals and start-up oriented engineering labs all over the country.

Virginia as a Connector

Virginia is unparalleled in helping private companies interface and develop cross-industry relationships with military and federal government entities through its proximity to the nation's capital and to the Virginia-based Federally Funded Research and Development Centers (FFRDC) such as MITRE and the Aerospace Corporation; research consortiums such as the Commonwealth Center for Advanced Manufacturing (CCAM) and the Commonwealth Center for Advanced Logistics Systems (CCALS); government research organizations such as NASA; and the Virginia Cyber Security Partnership. By addressing a variety of industries and involving private and public entities, Virginia's ecosystem of innovation is driving the frontier of cyber security technologies as no other state can. Governor McAuliffe's focus on cyber security development across the nation as Chair of the National Governors Association is a direct result of the success of Virginia's approach.

The Commonwealth of Virginia recognizes its role as the partnering force between the federal government and private industry to accomplish the vital task of supporting American interests throughout the world and to provide the workforce, education, infrastructure, and pro-business environment to help those partnerships flourish. The federal government, led by the February 2016 initiative to invest over $19 billion for cyber security as part of the President's Fiscal Year (FY) 2017 Budget—a 35% increase from FY 2016—represented the continued growth in support and need.[47]

More recently, a Cybersecurity National Action Plan (CNAP), and an additional $3.1 billion to modernize, retire, or replace outdated IT infrastructure characterizes the federal support for cyber security issues. The CNAP also routes an additional $62 million for cyber security personnel, especially those at the National Centers for Academic Excellence Cybersecurity Program locations including George Mason University, Hampton University, James Madison University, Lord Fairfax

[47]https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Community College, Marymount University, Norfolk University, Northern Virginia Community College, Radford University, Tidewater Community College, and Virginia Polytechnic Institute and State University—all located in the Commonwealth of Virginia.[48]

Beyond those institutions within Virginia that are heavily involved with the federal government already, Virginia seeks to be a home for new developing technology partnerships such as the newly envisioned Cybersecurity Assurance Program, National Center for Cybersecurity Resilience, and to be a leading voice in the public-private partnerships between technology companies and government envisioned by the White House in February 2016.[49] The federal government has signaled their long-term interest in partnering with states that are pro-business, locally accessible to help reduce logistical costs, and able to meet the current and future challenges facing the country. Private industry has also shown interest in investing in cyber security technologies, estimating a market size of $77 billion in 2015 with growth to $170 billion by 2020 through active participation by venture capital and new accelerator program development in Virginia.[50]

The Northern Virginia area, specifically, is the "best positioned in the nation to be the next 'Silicon Valley' of cyber security as it combines a developing workforce... advanced and modern infrastructure... and proximity to end-users."[51] By combining access to the national epicenter of security technology needs, proximity to 19 defense installations, and a refocusing on security procurement at the national level, Northern Virginia and the rest of state is directly competing with other traditional technology hubs on the West Coast.

It will take true leadership, partnership, and support from government to meet the new challenges brought on by technologies cultivated today and Virginia is setting the benchmark for innovative solutions. IoT is expected to bring on new challenges and "lift cyber security spending and research through 2025... while a cyber security workforce shortage is expected to reach 1.5 million unfilled positions by 2019."[52] Virginia is ahead of the game, addressing both needs through the creation of industry-led accelerator programs, academic and private research oriented collaborations, and heavy investment in the public university system cultivating tomorrow's leaders, today. Virginia's Centers of Excellence for Education in Cyber Security, Centers of Excellence for Research in Cyber Security, and Scholarship for Service where cyber security students earn federal financial assistance are sterling demonstrations of Virginia's leadership in education solving the needs of industry.[53]

[48]https://www.iad.gov/NIETP/reports/current_cae_designated_institutions.cfm
[49]https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf
[50]http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#1ff1b58710b2
[51]http://passcode.csmonitor.com/goldrush
[52]http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/3/#15e47bfb26f9
[53]https://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf

Cyber Security: Enabling & Protecting the Innovation Ecosystem

The Commonwealth does not see cyber security as a technology industry that stands alone, but as a partner in the innovative landscape for the future that the governor's office has worked diligently to cultivate. Virginia is now a world leader in the field of Unmanned System Technologies (UMS) throughout ground, air, sea, and space and leads the nation as one of only eight FAA designated test-sites in the United States—the Mid-Atlantic Aviation Partnership (MAAP). MAAP's Virginia lead is Secretary of Technology Karen Jackson who also co-chaired the Virginia Cyber Security Commission which outlined the state's policies and goals for cyber security initiatives and needs.

Both industries have similar problems and needs, and with leadership involved in both initiatives private companies have a knowledgeable and involved executive with whom to align their own expectations. The UMS industry considers cyber security one of the most important elements in enabling future developments and integration into commercial operations. The FAA, AUVSI, and other stakeholders all cite communications protection, data and privacy security, and signal assurance as necessary to success in unmanned

robotics. These technologies must grow together and industry relationships developed in Virginia will enable that growth with significant efficiency and effectiveness. The latest news in the Unmanned Aircraft Systems (UAS) industry is the regulatory steps forward allowing for commercial operations legally in the United States. This makes investment, business planning, and innovation much easier for UAS as uncertainty is diminished. New regulations are on the way for the UAS industry, just as Virginia evolves its multi-domain robotics support. By supporting these UMS industries with regional innovation and application of cyber security, Virginia pushes the limit for where both technology industries can go.

Virginia as a Partner

The Commonwealth Research Commercialization Fund and the Center for Innovative Technologies (CIT) are key players in promoting homegrown innovation for any investment opportunities. This center, developed as a flagship for the new Virginian economic development plan, thrives in the recognition that the availability of early-stage capital is a critical need of many emerging technology companies and that making connections with private, public, and international funding is a difficult step in the start-up lifecycle.[54]

CIT has created for any early-stage start-up the Commonwealth Innovation and Entrepreneurship Measurement Systems (IEMS), a web-based portal using key metrics to track the performance of Virginia's innovation economy, allowing angel investors and private equity firms and other stakeholders a unique insight into the life-cycles and stages of start-up companies in Virginia along with opportunities to get involved very easily. This reduces the hurdles of engagement for investment for companies and investors alike.[55]

Small businesses have been rewarded significantly by beginning their journey in Virginia. The Small Business Innovation Research (SBIR) program and the Small Business Technology Transfer program (STTR) offer similar incentives for small business that partner with non-profit research institutions. Virginia based firms, because of the local and supported access to non-profit organizations such as universities, military and non-military government groups, and R&D laboratories received a total of $109.6 million in SBIR/SBTT funds in 2014, the third highest amount of any state.[56]

By focusing on all levels of a company's life cycle, Virginia provides the perfect environment to start, grow, and commercialize any cyber-related firm. By taking advantage of the unique characteristics and government support provided in Virginia, companies make a smart decision for their future. ■

[54]http://www.cit.org/service-lines/cit-entrepreneur/
[55]http://www.cit.org/initiatives/iems/measurement-system/
[56]http://www.cit.org/initiatives/iems/research-and-development/

Incentives

New Virginian companies can be supported by unique incentives geared toward enabling technologies in sub-markets. While this has created a friendly environment for all business development within the state for new or expanding firms, there are number of technology-focused programs of which to be aware.

Commonwealth's Opportunity Fund

The Commonwealth's Opportunity Fund (COF) is a discretionary incentive available to secure a business location or expansion project for Virginia. Grants are awarded to localities on a local-matching basis with the expectation that the grant will result in a favorable location decision for the Commonwealth.

Grant requests are made by the community for a project under the following conditions:

- Projects must meet investment, job creation, and wage minimums
- Matching local financial participation is required on a dollar-for-dollar basis (cash or in-kind)
- Public announcement of the project must be coordinated by the Virginia Economic Development Partnership and the Governor's Office (neither the company nor the locality may publicly confirm the proposed project)
- Grants are made at the discretion of the Governor

http://www.yesvirginia.org/ProBusiness/BusinessIncentives

Governor's Development Opportunity Fund

The Governor's Development Opportunity Fund (GOF) provides either grants or loans to localities to assist in the creation of new jobs and capital investment in accordance with criteria established by legislation.

General Eligibility Thresholds:

- 50 new jobs / $5 million capital investment; or
- 25 new jobs / $100 million capital investment

The average annual wage for the new jobs must be at least equal to the prevailing average annual wage in the locality, excluding fringe benefits. If the average annual wage is twice the prevailing average annual wage, the Governor may reduce the new jobs threshold to as low as 25.

http://www.virginiaallies.org/assets/files/incentives/GOFGuidelines.pdf

Virginia Investment Partnership Act/Major Eligible Employer Grant

The Virginia Investment Partnership (VIP) Grant and the Major Eligible Employer Grant (MEE) are designed to encourage continued capital investment by Virginia companies. This is intended to add capacity, modernize, increase productivity, creation, development, and utilization of advanced technology. UMS technologies are specifically being targeted for this type of investment.

To be eligible for a VIP grant, a minimum of $25 million in capital investment is required by an eligible existing Virginia manufacturer or research and development service.

http://www.virginiaallies.org/assets/files/incentives/VIPGuidelines.pdf

The Virginia Economic Development Incentive Grant

The Virginia Economic Development Incentive Grant Program (VEDIG) assists and encourages companies to invest and to provide new employment opportunities by locating significant headquarters, administrative, research and development, and/or similar service and basic sector operations in Virginia. This is a discretionary program in which grants are negotiated and offered to qualified applicants as an economic development incentive.

The VEDIG program has two separate eligibility requirements. Companies located in a Metropolitan Statistical Area with a population of 300,000 or more in the most recently preceding decennial census, must:

- Create or cause to be created and maintained (i) at least 400 jobs with average salaries at least 50% greater than the prevailing average wage; or (ii) at least 300 jobs with average salaries at least 100% greater than the prevailing average wage
- Make a capital investment of at least $5 million or $6,500 per job, whichever is greater. For all companies located elsewhere in Virginia, the company must create or cause to be created and maintained at least 200 jobs with average salaries at least 50% greater than the prevailing average wage, and make a capital investment of at least $6,500 per job

http://www.virginiaallies.org/ assets/files/ incentives/VEDIGGuidelines.pdf

Tobacco Region Opportunity Fund

The Tobacco Region Opportunity Fund is available to tobacco producing regions to assist with specific projects that result in the creation of new jobs and investment. Grants are made to the community at the discretion of the Tobacco Region Revitalization Commission. The goal of the fund is to attract competitive projects expected to have a regional impact due to the magnitude of new employment and investment, and the possibility of follow-on industry.

- Evaluation of award amount is consistent throughout the region and is based on the following criteria: local unemployment rates, prevailing wage rates, number of new jobs, capital investment levels, industry type, and the possibility of related economic multiplier effect
- TROF is the only Tobacco Commission grant program paid at the beginning of the project to help tobacco region localities be competitive in attracting new investment and jobs resulting in increased tax revenue and opportunity for quality employment in the tobacco region
- Intended to support the goal of the Commission to "revitalize the economies of tobacco-dependent regions and communities." This goal is measured by job creation, workforce participation rate, wealth, diversity of economy, and taxable assets. All measurements listed are increased when a new or expanding business in the tobacco region creates new jobs that pay more than prevailing wage and adds taxable assets to the local tax rolls

http://www.tic.virginia.gov/tobregionoppfund.shtml

Center for Innovative Technology Incentives

Commonwealth Research Commercialization Fund

The Commonwealth Research Commercialization Fund (CRCF) accelerates innovation and economic growth in Virginia by advancing solutions to important state, national, and international problems through technology research, development, and commercialization. Cyber security has been identified as a critical field of study.

Proposals submitted to CRCF undergo a multi-stage review process, which includes award recommendations made by the Research and Technology Investment Advisory Committee (RTIAC) to the CIT Board of Directors and culminates with award decisions made by the Board. CRCF awards contribute to the Commonwealth's overall plan to enhance economic development through technology research and commercialization and, as such, CRCF awards must further the goals set forth in the Commonwealth Research and Technology Strategic Roadmap. In addition to identifying research areas worthy of economic development and institutional focus, the Roadmap provides a framework for aligning key industry sectors within the state, as prioritized by the research community, which includes but is not limited to the private sector, academia, and economic development professionals.

http://www.cit.org/initiatives/crcf/

CIT GAP Funds

CIT GAP Funds is a family of seed and early-stage investment funds placing near-equity and equity investments in Virginia-based technology, life science, and clean tech companies. CIT GAP Funds invests in companies with a high potential for achieving rapid growth and generating significant economic return for entrepreneurs, co-investors and the Common-wealth of Virginia.

CIT's family of funds includes:

- GAP Fund I – A vintage 2004 fund fully invested in a broad array of seed-stage technology companies
- GAP BioLife Fund – A seed fund investing exclusively in life science companies
- GAP Tech Fund – A seed fund investing in IT and technology companies
- Commonwealth Energy Fund (CEF), a seed fund investing in energy efficiency and renewable energy companies

http://www.cit.org/service-lines/cit-gap-funds/

CIT GAP Tech Fund

The CIT GAP Tech Fund makes seed-stage equity investments in Virginia-based technology companies with a high potential for achieving rapid growth and generating significant economic return. The fund invests exclusively in companies headquartered, and with an express desire to grow in the Commonwealth of Virginia.

Sectors (includes cyber security)

- Software, Telecommunications
- Semiconductors
- Security
- Information and Communication

Technologies

- E-Commerce
- Networking and Equipment
- Electronics/Instrumentation
- Computers and Peripherals
- Sensors
- Materials

http://www.cit.org/service-lines/gap-tech-fund/

Business Development Tax Credits

Refundable Research and Development Expenses Tax Credit

This credit is an individual and corporate income tax credit for certain taxpayers that incur Virginia qualified research and development expenses.

During the 2014 Session, the Virginia General Assembly enacted legislation that increased the overall credit cap, increased the per taxpayer credit cap, allows pass-through entities to elect to claim the credit at the entity level, and requires taxpayers to provide certain information to the Department of Taxation ("the Department") when applying for the credit.

http://www.tax.virginia.gov/content/rd

Enterprise Zone Tax Credit

This credit provides state and local incentives to businesses that invest and create jobs within Virginia's enterprise zones, which are located throughout the state.

http://www.tax.virginia.gov/content/tax-credits#enterprise

Major Business Facility Job Tax Credit

Through this credit qualified companies locating or expanding in Virginia receive a $1,000 income tax credit for each new full-time job created over a threshold number of jobs.

- Companies locating in Enterprise Zones or economically distressed areas are required to meet a 25-job threshold; all other locations have a 50-job threshold. The threshold number of jobs must be created within a 12-month period
- The $1,000 credit is available for all qualifying jobs in excess of the threshold and is taken in equal installments over two years ($500 per year) through 2014. Credits earned after 2014 will be taken in equal installments over three years
- Non-qualifying jobs include seasonal positions shifted within Virginia, building and grounds maintenance, security, and other positions ancillary to the principle activities of the facility
- Credits are available for taxable years before January 1, 2020. Unused credits may be carried over for up to 10 years

http://www.tax.virginia.gov/content/tax-credits#Major_Business_Facility_Job_Credit

Qualified Equity And Subordinated Debt Investments Credit

This credit offers angel investors a 50% tax credit for pre-qualified small business ventures involved in technology fields. The state also offers individual and corporate income tax subtractions for long-term capital gains attributable to qualified investments in early stage technology, biotechnology, and energy start-ups; technology, nanotechnology, or any similar technology-related field, which includes cyber security.

- The credit is equal to 50% of the qualified business investments made during the taxable year. If total annual requests for the credit exceed $5 million for tax year 2015, the Department of Taxation will prorate the credit for each taxpayer
- The credit a taxpayer may claim per taxable year may not exceed the credit authorized by the Department of Taxation, $50,000, or the income tax liability on that year's return, whichever is less. The credit is nonrefundable. Unused credits may be carried forward up to 15 years

http://www.tax.virginia.gov/content/tax-credits#Qualified_Equity_And_Subordinated_Debt_Investments_Credit

Telework Expenses Tax Credit

This credit allows a tax credit to employers for eligible expenses incurred for allowing employees to telework pursuant to a signed telework agreement for taxable years beginning on or after January 1, 2012, but before January 1, 2017. An employer may be eligible for a credit of up to $1,200 per teleworking employee and/or a maximum of $20,000 for conducting a telework assessment.

- The telework assessment can only be allowed once. The aggregate amount of tax credits that will be issued is capped at $1 million annually
- An employer shall be ineligible for a tax credit pursuant to this section if such employer claims a credit based on the jobs, wages, or other expenses for the same employee under any other provision of this chapter. Additionally employers are not allowed to deduct expenses that are deducted for federal purposes

http://www.tax.virginia.gov/content/tax-credits#TeleworkExpensesTaxCredit

Worker Retraining Tax Credit

This credit allows an employer to claim a tax credit for the training costs of providing eligible worker retraining to qualified employees for taxable years beginning on or after January 1, 1999. The credit may be applied against individual income tax, estate and trust tax, corporate income tax, bank franchise tax, and taxes imposed on insurance companies and utility companies.

Eligible worker retraining includes noncredit courses approved by the Virginia Economic Development Partnership. For information on noncredit course approval, call (804) 545-5706. It also includes credit or non-credit retraining courses undertaken through an apprenticeship agreement approved by the Commissioner of Labor and Industry.

The credit is generally 30% of all classroom training costs:

- Limited to up to $200 annual credit per student if the course work is incurred at a private school or $300 per qualified employee with retraining in a STEM or STEAM discipline
- The Department of Taxation is authorized to issue up to $2,500,000 of retraining credits annually. If total requested credits exceed this amount, the Department of Taxation will prorate the authorized credits
- Credits taken may not exceed tax liability in any one taxable year. Unused credits may be carried forward for three years

http://www.tax.virginia.gov/content/tax-credits#Worker_Retraining_Credit

Additional Tax Credits

Sales and Use Tax Exemption

This exemption is for purchases used exclusively in research and development.

Research and Development Tax Credit

Businesses may claim a tax credit equal to 15% of the first $234,000 in Virginia qualified research and development expenses incurred during the taxable year or they may claim a tax credit equal to 20% of the first $234,000 in Virginia qualified research and development expenses if the qualified research was conducted in conjunction with a Virginia college or university.

- $6 million cap on the total amount of credits allowed in any fiscal year

http://www.tax.virginia.gov/content/tax-credits#ResearchandDevelopmentTaxCredit

Credit for Tax Paid to Another State

The Code of Virginia makes out-of-state tax credit provisions for income taxed by more than one state. The credit is restricted to certain types of income. The intent of the law is to address double taxation when income is generated in more than one state; however, the credit does not eliminate double taxation in all cases. For example, taxes paid to another state on non-qualifying income would not be subject to the credit provisions.

Generally, Virginia will allow taxpayers filing resident individual income tax returns to claim credit for income tax paid to another state on qualifying income derived from sources outside of Virginia, provided the income is taxed by Virginia as well as the other state. If the income is from one or more of the following states, the credit should be claimed on the nonresident income tax return of the other state instead of the Virginia return: Arizona, California, District of Columbia, Oregon.

http://www.tax.virginia.gov/content/tax-credits#Credit_for_Tax_Paid_to_Another_State

Programs

SSBCI Virginia Capital Access Program

This program provides loan loss insurance to a bank to cover a portfolio of enrolled loans. It is designed to be a quick, efficient means of obtaining a credit enhancement from the VSBFA. Under most circumstances, the bank determines whether a loan will be enrolled in the program without VSBFA's involvement.

- Program is designed to assist financial institutions in making small business loans by mitigating some of the risk associated with the loan
- Program offers lenders a flexible, non-bureaucratic tool to expand their market base and enhance their ability to meet the financing needs of Virginia's businesses

http://www.vabankers.org/ssbci-virginia-capital-access-program

Small Business Microloan Program

This is a direct loan from the VSBFA to the business client that does not require a bank's participation in the transaction. It is an ideal tool for bankers who are faced with business loan requests for very small amounts where the bank would prefer to refer the client to an alternative source of funds.

The Virginia Small Business Financing Authority (VSBFA) is the Commonwealth of Virginia's economic development and business financing arm and helps banks make loans to businesses that can demonstrate repayment ability, but where the bank needs additional collateral support or a more robust secondary repayment source by providing:

- Cash collateral
- Subordinate companion loans
- Guaranties
- Loan loss reserves

http://www.vabankers.org/VSBFA

Economic Development Access Program

Administered by the Virginia Department of Transportation, this program assists localities in providing adequate road access to new and expanding basic employers.

- Funds may be used for financing the construction or improvement of secondary or local system roads within all counties and cities, and certain towns that are part of the Urban System, hereinafter referred to as eligible localities
- Ancillary improvements, such as turn lanes or intersection modifications may also be warranted as part of the access project, but are not considered the primary objective of the project

http://www.virginiadot.org/business/resources/local_assistance/access_programs/EconomicDevelopmentAccessProgramGuide.pdf

Zones

Enterprise Zones

The Virginia Enterprise Zone (VEZ) program is a partnership between state and local government that encourages job creation and private investment. VEZ accomplishes this by designating Enterprise Zones throughout the state and providing two grant-based incentives, the Job Creation Grant (JCG) and the Real Property Investment Grant (RPIG), to qualified investors and job creators within those zones, while the locality provides local incentives.

State incentives are available to businesses and zone investors who create jobs and invest in real property within the boundaries of enterprise zones.

http://www.dhcd.virginia.gov/index.php/community-partnerships-dhcd/downtown-revitalization/enterprise-zone.html

Enterprise Zone Job Creation Grant

Job Creation Grants are based on net new permanent full-time job creation exceeding a four-job threshold. Positions over the four-job threshold must meet wage and health benefits requirements to be eligible for the JCG. Firms can receive grants for up to 350 positions per year.

- Business firm must be located in a Virginia Enterprise Zone
- Business firm must create at least 4 net new permanent full-time positions over the base calendar year
- Net new permanent full-time positions created over the 4-job threshold must meet wage (at least 175% of the Federal Minimum Wage, 150% in High Unemployment Areas) and health benefits requirement (at least 50% of employee's premium paid for by employer)
- Grants are available for a five-consecutive-year qualification period
- To be eligible for the JCG in years 2-5 of the grant cycle, a business firm must maintain or increase the number of eligible permanent full-time positions (above the 4-job threshold) over base year employment. Base year employment levels are established during the first grant year and will remain consistent throughout the 5-year grant period
- Firms can continue to receive grants for any net new permanent full-time positions created over base year employment levels that meet wage and health benefits requirements
- Firms may apply for a subsequent 5-year period given they meet the grant eligibility requirements. Grant Year 2011 was the first year firms were eligible to begin subsequent five-year periods

http://www.dhcd.virginia.gov/images/VEZ/JCG-Instruction-Manual.pdf

Enterprise Zone Real Property Investment Grant

Real Property Investment Grants are available for investments made to industrial, commercial, or mixed use properties located within the boundaries of Enterprise Zones. Grants are available to qualified zone investors in amounts up to 20% of the qualified real property investment, not to exceed $200,000 per building or facility within a five year period.

The property (building or facility) must be located within the boundaries of a Virginia Enterprise Zone:

- The building or facility must be commercial, industrial, or mixed-use. Mixed-use is defined as a building incorporating residential uses in which a minimum of 30% of the usable floor space is devoted to commercial, office, or industrial use
- For the rehabilitation or expansion of an existing structure, the zone investor must spend at least $100,000 in qualified real property investments to be eligible
- For new construction projects, the zone investor must spend at least $500,000 in qualified real property investments to be eligible
- Grants may not exceed $200,000 per building or facility in a 5 consecutive-year period. 5-year periods being with the qualification year in which a grant was first awarded
- After the conclusion of a 5-consecutive-year period, the property beings another eligibility period and the grant cap of $200,000 is restored

http://www.dhcd.virginia.gov/images/VEZ/RPIG-Instruction-Manual.pdf

Technology Zones

Virginia authorizes its communities to establish technology zones to encourage growth in targeted industries. Presently, 30 cities and counties and 6 towns have created zones throughout the state. Qualified businesses locating or expanding operations in a zone may receive local permit and user fee waivers, local tax incentives, special zoning treatment, or exemption from ordinances. Once a local technology zone has been established, incentives may be provided for up to 10 years.

Localities that have established technology zones include the counties of Amherst, Arlington, Bedford, Caroline, Chesterfield, Culpeper, Fauquier, Frederick, Halifax, Henry, Page, Roanoke, Rockingham, Russell, Smyth, Spotsylvania, Stafford and Warren; the cities of Buena Vista, Charlottesville, Chesapeake, Falls Church, Franklin, Fredericksburg, Harrisonburg, Lynchburg, Manassas, Manassas Park, Newport News, Poquoson, Suffolk and Winchester; and the towns of Ashland in Hanover County, Bridgewater in Rockingham County; Cape Charles in Northampton County, Front Royal in Warren County, Kilmarnock in Lancaster County, Marion in Smyth County and Wytheville in Wythe County.

http://www.virginiaallies.org/assets/files/incentives/techzonewriteup.pdf

Foreign Trade Zones

Foreign Trade Zones (FTZ) are areas which are geographically inside the United States, but are legally considered outside its Customs territory. Companies that locate in FTZs can benefit by using special procedures to encourage U.S. activity by reducing, eliminating, or delaying duties.

- Virginia offers 6 foreign trade zones designed to encourage businesses to participate in international trade by effectively eliminating or reducing customs duties
- Numerous subzones are provided and additional ones can be designated to enhance the trade capabilities of specific companies and technologies such as UMS

http://www.yesvirginia.org/ProBusiness/BusinessIncentives

Defense Production Zones

Virginia's cities, counties, and towns have the ability to establish, by ordinance, one or more defense production zones to attract growth in targeted industries. Establishment of a defense production zone allows localities to create special incentives and certain regulatory flexibility for qualified businesses locating or expanding operations in a zone. These incentives may include: reduction of user and permit fees, special zoning treatment, exemption from local ordinances or other incentives adopted by ordinance. Virginia authorizes its communities to establish local defense production zones to benefit businesses engaged in the design, development, or production of materials, components, or equipment required to meet the needs of national defense. Companies deemed ancillary to or in support of the aforementioned categories would also apply.

- Once a defense production zone is established, incentives may be provided for up to 20 years
- Each locality designs and administers its own program
- Establishment of a defense production zone shall not preclude the area from also being designated as an enterprise zone
- Two localities currently have an established Defense Production Zone:
  - Fauquier County and the City of Manassas Park;
  - Henrico County will create individual defense production zones based around individual projects on a case-by-case basis

http://www.vaallies.org/assets/files/incentives/defenseproductionzoneswriteup.pdf

Conclusion

Virginia is proud of its distinguished history and exemplary record of national leadership through exceptional cyber security operations in support of state agencies and operations. The Commonwealth is resolute in its dedication to garnering the expertise of leaders in cyber security in order to mitigate risks. By ensuring the highest level of security for government infrastructure networks, fostering cyber security education and awareness, incorporating innovative best practices to protect data statewide, bolstering business investment with public-private partnerships, and proactively enhancing its national standing as one of the preeminent leaders in the cyber security arena, the Commonwealth leads the nation for cyber security policy.

It's also clear that the Commonwealth of Virginia has developed a world leading technology ecosystem founded on private industry innovation and public-private partnerships. Reflected in the strong presence of state, federal, military, and private cyber security businesses, assets, and activities throughout the Commonwealth, Virginia has leveraged its unique resources and relationships to create this ecosystem of innovation that underpins thriving industry development. Leaders from business, government, and higher education have joined in a shared vision that the Commonwealth will not only continue to lead the nation in the adoption of signature Information Communication Technologies (ICTs), but to formulate and promote their creation through innovation, investment, and a pro-business environment that nurtures all companies.

The Commonwealth stands as an able and active partner that facilitates the types of innovation that have made the Commonwealth the home of the top technology companies and the number one recipient of federal investment. A shared vision for pro-business policies, a highly skilled workforce, a world-class education system, and cutting-edge technology research have put Virginia squarely at the forefront of cyber security.

Innovation and rapid technology change dominate all markets and all networks, providing ample opportunities for attack, malicious activities, and the degradation of the very systems needed to support society in this interconnected world. The Commonwealth of Virginia understands the devastating impact that neglecting these cyber security challenges poses, and has made it a primary goal to provide an environment for leaders to find partners, companies to find infrastructure and investment, and adversaries to find impenetrable defenses. ■

cyberva.virginia.gov