Cyber Commission Final Report

The Virginia Cyber Commission concluded its activities on 29 March 2016 after two years of focused action to enhance the overall security posture of Commonwealth information technology systems, rapidly develop a Virginia cyber workforce through innovative education programs, increase the overall cyber knowledge and resilience of Commonwealth citizens, modernize Commonwealth statute and law enforcement capabilities to address the rapidly changing cyber environment, and build on Virginia's existing cyber and technology industry to bring new cyber related industries and jobs to the Commonwealth. Nine Commission meetings, several working group sessions, nine Town Hall events, and countless hours of Commission and volunteer staff effort generated a broad range of recommendations that have led to numerous actions that directly support the founding objectives of the Commission. 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). This report highlights the activities and actions of the Commission since the publication of the August 2015 recommendations. This document also makes specific recommendations for areas of continued emphasis. *Note: References to recommendations are denoted with the commission working group abbreviation followed by the recommendation number. Example: Infrastructure recommendation one will be referenced as (CI-1).*

Commonwealth Cyber Infrastructure and Network Protection. Numerous recommendations have been championed by the Governor's office with support from the General Assembly to strengthen the overall levels of cyber security and resilience of the Commonwealth's broad and diverse information systems. The Secretaries of Technology and Public Safety and Homeland Security have successfully led the charge on many of these initiatives. Including cyber security and data protection as a key duty for all Commonwealth agency heads[1] has helped foster the proactive environment necessary to make significant progress in protecting the Commonwealth's critical data. This environment has allowed the following initiatives to come to fruition since the first report.

a. Establishment and funding of a shared service to provide cyber security services and implement data protection protocols at Commonwealth agencies. This task was undertaken as a result of information gathered under Cyber Infrastructure Recommendation Two (CI-2), "Accelerate Adoption of Identity Access Management and Encryption."[2] This initiative will help standardize and enhance the methodologies used to protect the Personally Identifiable Information (PII) the Commonwealth manages each and every day. This, along with significant enhancements in Identity Access Management (IAM) will reduce the levels of risk inherent with processing and storing large amounts of PII. This initiative will be challenging given the broadly varying levels of cyber maturity of Commonwealth

[1] Establishing Data security responsibilities for agency heads was a year-one Commission recommendation codified by legislation passed during the 2015 GA session (SB1121).

agencies, take time to complete, and likely require additional resources in the future as threat vectors constantly change. Continued focus on this specific area will be needed to maintain momentum and progress being made in this extremely important area.

b. Establishment and funding of a Cyber Security Architect position for the Virginia Information Technology Agency is another forward leaning initiative that will directly support the PII protection and IAM initiatives from recommendation CI-2 as well as develop streamlined cyber capabilities and processes across all Commonwealth systems. [2]

c. Per recommendation CI-5 in the 2015 report, the Virginia National Guard has started conducting cyber assessments in several Virginia municipalities. [2] The assessments provide these entities with detailed reports on core cyber weaknesses that could threaten the integrity of the sensitive citizen and critical operational data that many municipalities and counties hold. These assessments are helping community leaders importantly prioritize remediation. The Commission believes that this initiative should be expanded. Also, this practice should be championed by the National Governors Association for potential federal funding in each state.

d. As recommended in CI-1, the Commission strongly supports the establishment of a Joint Cybersecurity Operation Center (JCSOC) that would centralize all of the cyber resources of the Commonwealth into one physical environment where unity of effort, cross training, shared situational awareness, and streamlined communications can be generated. [2] The Commission realizes that making the JCSOC a reality is a significant lift but the benefit far outweighs the cost. The Commission recommends that the establishment of the JCSOC remain a high priority item.

e. Establishment of a Virginia Information Sharing and Analysis Organization (ISAO) is another area where the Commission recommends continued focus. This initiative is included in the Center for Innovative Technology's 2017 budget. The ISAO is intended to serve as the link that aligns many of the initiatives, especially in the infrastructure arena. The ISAO will become the primary mechanism where municipalities, counties, critical infrastructure, and businesses can share and receive cyber threat information and strategies.

f. During the Commission's final meeting, a recommendation was advanced that the Commonwealth develop and conduct a regular Cyber incident program to conduct response training exercises with the intent of making the entire Commonwealth more secure. Both internal (breach of PII) and external (major private critical infrastructure breach) scenarios should be routinely undertaken. This important work was pursued under the umbrella of Public Awareness Recommendation One (PA-1). [2]

Education and Workforce Development. During our analysis and discussions on the main focus areas, the Commission concluded that education would serve as the catalyst for many of these areas. Economic development, Commonwealth infrastructure improvements, and public awareness are all highly dependent on the growth and maintenance of a robust cyber workforce. Understanding this critical linkage resulted in numerous Commission recommendations to accelerate the development of a sustainable workforce pipeline capable of developing, attracting and sustaining cyber companies, defending critical Commonwealth assets, and creating a more cyber-aware citizenry. These culminating recommendations and actions are a result of collaboration between the Commission, the Secretary of Technology, the Secretary of Education, and the Secretary of Commerce and Trade. Resulting initiatives and continued areas of focus include:

a. Need for funding to expand STEM summer camps for teachers and guidance counselors. Based on numerous presentations to the Commission from professional educators and organizations directly supporting expanded STEM education, the Commission is convinced that educating teachers on methodologies to excite our youth to pursue STEM training is integral to creating the interest pool needed to maintain an expansive cyber workforce. This conclusion draws upon data accrued based on research stemming from Education and Workforce Recommendation Eight (ED-8), "Expand Cyber Educational Opportunities and Experiences for Virginia Teachers and Guidance Counselors."[2]

b. Encouraging Virginia's youth to seek STEM education and careers is essential to expanding the cyber workforce. Based on Commission recommendations, the Governor's Office supported SB246 (2016), a bill that establishes a STEM Competition Team Grant Program. This bill is crucial because it allows students of all financial backgrounds to gain exposure to the STEM world. This initiative in concert with exciting after school "hands on" programs like First Robotics, Cyber Patriot, U.S. Cyber Challenge, and VEX are the right steps to building the needed base of interested students that are well prepared to pursue post-secondary cyber education. Additional support in this area would likely have a profound impact on generating a Virginia technology workforce.

c. In accordance with ED-4, the Governor and his office were instrumental in obtaining funding to start a program the Virginia Cybersecurity Scholarship for Service. A program that emulates the Federal Scholarship for Service program. The new Virginia program promotes a desire to pursue cyber careers and public service by incentivizing post-secondary education in cybersecurity while also widening accessibility to the cyber world across socio-economic barriers. This will contribute to the number of high quality cyber professionals that the Commonwealth needs to operate and defend its critical technology systems.

d. Creation of and funding for a full time position to leverage Northern Virginia Community College experience in developing a nationally certified (CAE) Cyber Program and exporting it to other Virginia community colleges. This is a direct result of ED-2, "Obtain Certification for Additional Community Colleges."[2] Additionally, staffing has been provided to assist schools pursuing the CAE designation in developing and submitting successful accreditation packages. The Commission strongly believes that the most rapid way to create the necessary cyber workforce in the short term is through certified programs at these educational institutions. As a result of these efforts, three more Virginia post-secondary schools have been accredited this year, including two community colleges (Lord Fairfax CC and Tidewater Community CC and one four year institution (Radford University). Virginia's continued investment in this arena will exponentially increase the cyber talent pool that is in constant demand by this rapidly growing industry.

e. As illustrated in ED-6, "Create a shared, virtual Cyber Range for training purposes…,"a key component for a school to earn the CAE designation is having the capability to provide students with the "hands on experience" obtained from learning on the technology platforms and cyber tools currently used in today's enterprise environments.[2] Commonly referred to as a "cyber range", many smaller schools cannot afford the investment needed to build, operate, and maintain the complex technologies needed. In our first report, the Commission recommended the creation of a virtual cyber range operated by one of the major universities or a public-private consortium that could be used by numerous schools in a fast paced environment. The Commission is extremely pleased to see this initiative moving forward with a work group tasked to develop the requirements and funding assigned to support the development of the needed shared platform. These initiatives will eliminate a major obstacle in generating as many certified schools as possible.

f. Hosted the Inaugural Cyber Security Education Conference in December 2015 as recommended in ED-7.[2] This event was crucial in connecting the public and private sector in order to collaborate and develop more initiatives for the future that will benefit the Commonwealth and its Citizens.

g. The recent roll out of the Cyber Security Registered Apprentice program is applauded by the Commission and will be another aid in providing the cyber workforce sought by so many Virginia businesses. For more information, see: https://governor.virginia.gov/newsroom/newsarticle?articleId=15727

Public Awareness. Commission members traversed the Commonwealth to raise awareness about the initiatives and to receive crucial feedback. A total of nine Town Halls and forums were held throughout the state in order to directly engage with citizens, businesses, and public officials. The conclusion drawn from this feedback was that the people are concerned, but that they don't know how to take action. This direct feedback resulted in a Commission

recommendation to expand the Commonwealth Cyber Portal, which can be found at CyberVA.virginia.gov. This portal aggregates cyber related information in a centralized, user-friendly format that citizens and businesses can access. The Commission is extremely pleased to see the standup of the Cyber Portal on the cyberva.virginia.gov web page. Continued focus on portal content and promoting the portal as a key communication platform for the Virginia ISAO will ensure that this capability will continue to help generate cyber awareness and resilience of the Commonwealth as a whole.

Economic Development. The Commission strongly believes that all of the above recommendations and initiatives directly contribute to generating an environment conducive to rapid creation, continued growth, and sustainment of new cyber and technology related industries within the Commonwealth. The Commission generated several recommendations that are necessities in order to attract and create new cyber businesses within Virginia. These recommendations uniquely align with existing Virginia cyber expertise and capabilities that have been developed over the last several years. Recommendations and ongoing initiatives include:

a. As a result of ECON-6, "Unmanned Systems-Specific Initiatives," the Commission spurred the creation of the Unmanned Systems Consortium.[2] This public-private body, which continues its work, is focused on cyber security issues related to Unmanned Aerial Vehicles (UAV). This group is currently working to establish a Virginia based Center of Academic Excellence (CAE) in order to increase cyber security capabilities to secure critical UAV operations. The consortium has generated active participation from Virginia based resources such as Langley and Wallops who both possess much of the infrastructure required to support testing of new capabilities. Continued engagement and support of the Mid Atlantic Aviation Partnership will continue to generate broad interest and additional capabilities to rapidly grow a UAV cyber security industry within the Commonwealth.

b. During the last year, the Commission worked to support the development of a collaborative environment (including stakeholders from academia, public and private businesses, and Federal agencies) that is crucial for new cyber security businesses focused on addressing the existing and evolving weaknesses in a broad range of automated systems. The broad range of cyber threats against automobiles was demonstrated through several demonstrations involving the Virginia State Police. Developing cyber security capabilities for the automobiles that we operate today is extremely important; but reaches critical level as autonomous vehicles become a reality. Cyber issues within advanced manufacturing was also a focal point for the Commission Economic Development work group and generated similar strong interest from broad groups of stakeholders.

c. The Internet of Things (IoT) is a new reality that is growing at a rapid rate. Consequently, cyber security concerns are routinely put on the back burner so as not

to slow innovation. The Commission strongly believes that based on our work regarding the development of initial cyber security capabilities for UAV's, automobiles, and advanced manufacturing, that Virginia is well positioned to generate new cyber industries related to a large portion of the IoT, specifically cyber security for physical systems. The Commonwealth Conference on Cyber & Physical System Conference scheduled for 20-22 September 2016 in Newport News will accelerate the initial work conducted by the Commission.

Cyber Crime. The Commission, working closely with the Attorney General, Secretary of Technology, and Secretary of Public Safety and Homeland Security, continued to develop new legislation to modernize Commonwealth statutes to address the broad range of new challenges posed by the rapidly changing cyber environment. During its first year, the Commission was successful in generating a broad range of legislation that was strongly supported by Assembly sponsors leading to passage. The Commission, in its second year, leveraged a study conducted by George Washington Law School that compared Virginia cyber related statute to those of other states. The study demonstrated the need to address weaknesses in the burden of proof and penalties related to cybercrimes so the Commission worked to develop the needed statute changes to address the gaps. Successful legislation achieved as a result of Commission activities include:

2015:

- **HB1946/SB919**: Sealing of administrative subpoenas for electronic communications and social networking data
- **SB1307**: Clarifies language for search warrants for seizure, examination of computers, networks, and other electronic devices
- **SB1109** Virginia Freedom of Information Act (FOIA); open meeting exemptions; discussions relating to cybersecurity
- **SB1121**: Agency directors; IT responsibility
- **HB 1562/ SB814**: Electronic identity management; standards and liability
- **SB1129**: Virginia Freedom of Information Act; record exemption for public safety; cybersecurity

2016:

- **SB246:** STEM Competition Team Grant Program and Fund; established, created
- **SB645**: Consolidates FOIA exemptions regarding cyber security and critical infrastructure information and strengthens language to protect private sector critical infrastructure providers who wish to share sensitive information with state authorities
- **HB924:** Electronic communications; disclosure, verification and admissibility of content Internet communications content may be authenticated in a criminal case by an Internet Service Provider (ISP) via affidavit.

Cyber Crime legislation not passed during the 2016 General Assembly session that will require continued emphasis and Administration support includes:

- **HB 922** – Computer Trespass; increases penalty if government computer and computer used for public utilities. Penalties for computer trespass of a government or critical infrastructure computer raised from a Class 1 misdemeanor to a Class 6 felony.
- **HB 923** – Computer trespass; penalty. Changes burden of proof of computer trespass crimes from "malicious" to "intentionally deceptive means".
- **HB 1138** – RICO; computer crimes; penalties. Adds crimes under the Virginia Computer Crimes Act as qualifying offenses under the Virginia RICO Act.

The Commission is extremely pleased to see FY17 and FY18 funding for new cyber positions that the Commission identified as critical to the Commonwealth's ability to investigate and prosecute cybercrime. The positions funded in FY2017 and FY2018 for ten cyber-crime special agents for the High Tech Crimes Division as well as four Virginia Fusion Center Cyber Analysts not only enhance the ability to prosecute crimes but also represent an enhanced response capability for internal and external cyber incidents. These positions will greatly assist law enforcement address the exponential growth in cyber evidence related to traditional crimes, provide the needed resources to start addressing the explosive growth in cybercrimes, and will be central to investigating any breaches of Commonwealth systems. This important investment in personnel and capabilities will likely require additional resources to educate the professionals on the latest cyber threats, forensics techniques, and new tools that they will need to remain relevant in this ever-changing field.

Areas of Continued Focus.

Recommendations from the Commission's first report that require further work are: [2]

For Commonwealth Cyber Infrastructure and Network Protection:

CI-3: Accelerate Adoption of a Common Cyber Security Guidance Framework
CI-4: Create a voluntary cyber security professional register and the Virginia Cyber Corps to assist local jurisdictions and school districts
CI-6: In conjunction with the Secretary of Public Safety and Homeland Security, and expertise from the Secretary of Veterans and Defense Affairs, develop pilot projects to improve security of control systems for the delivery of critical infrastructure services to military bases and installations throughout the Commonwealth.

Education and Work Force Development:

ED-1: Extend Northern Virginia Community College (NVCC) Program
ED-3: Expand the number of Public Universities certified as Academic Centers of Excellence in Cyber Security Education
ED-5: Develop a Student Outreach Program for Cyber Security Education
ED-7: Create the Virginia Cyber Security Education Forum

Economic Development

ECON-2: Support cross-sector research funding
ECON-3: Encourage new company formation
ECON-4: Leverage Industry Associations to build a cross-industry strategy for advanced manufacturing
ECON-5: Advanced Automation for Automobile-Specific Initiatives and Cyber-Physical Systems

The Commission's Recommendations would not have come to fruition without the strong support it received from the Office of the Governor and the Virginia General Assembly. The Commission has made lasting progress and made recommendations on many of the Commonwealth's cybersecurity-related challenges and opportunities. While significant progress has been made, there are many recommendations that require future attention and support as outlined in this document. As a final recommendation, the Commission recommends that cybersecurity remain a key focus area for the remainder of the current Administration and beyond. Policy and government often lag behind technology and the Commonwealth must remain both open-minded and vigilant to maintain its leadership position in this dynamic field.