Commonwealth of Virginia Cyber Commission
First Year Report

"Threats and Opportunities"

Executive Order Number 8

- Identify high risk cyber security issues facing COV.
- Provide advice and recommendations to secure COV networks, systems, and data.
- Suggest cyber security elements for COV Emergency Mgmt and Disaster Response capabilities.
- Offer suggestions for promoting Cyber awareness for citizens, business, and government entities.
- Present recommendations for educational & training programs to create a pipeline of cyber security professionals.
- Offer strategies to advance private sector cyber security economic development opportunities throughout COV; assess opportunities for private sector growth as it relates to military facilities and defense activities.

"Make this Commonwealth the world's leader in Cyber Security" Governor Terry McAuliffe

Core Commission Members

- **Richard Clarke**, Co-Chair, Chairman & CEO Good Harbor Security Risk Management.
- **Karen Jackson**, Co-Chair, COV Secretary of Technology
- **John Harvey**, COV Secretary of Veterans and Defense Affairs
- **Anne Holton**, COV Secretary of Education
- **Dr. Bill Hazel**, COV Secretary of Health and Human Resources
- **Maurice Jones**, COV Secretary of Commerce and Trade
- **Brian Moran**, COV Secretary of Public Safety and Homeland Security
- **Rhonda Eldridge**, Director of Engineering, Technica Corporation
- **Jennifer Bisceglie**, President and CEO Interos Solutions Inc

Core Commission Members

- **Dr. Barry Horowitz**, Munster Professor and Chair of Systems and Information Engineering Department, University of Virginia
- **Paul Tiao**, Attorney and Partner at Hunton and Williams LLP
- **Andrew Turner**, Vice President and Head of Global Security, VISA
- **Jeffrey Dodson**, Global Chief Information Security Officer, BAE Systems
- **Jandria Alexander**, Principal Director of Cyber Security, Aerospace Company
- **Elizabeth Hight**, Rear Admiral USN (ret), prior deputy DISA and VP Hewlett Packard Public Sector Cyber Security Practice.
- **John Wood**, CEO and Chairman of the Board, Telos Corp.
- **Paul Kurtz**, Chief Strategy Officer at CyberPoint

Cyber Infrastructure and Commonwealth Network Protection

Paul Kurtz – Chair
Betsy Hight
JC Dodson
SEC Bill Hazel

Volunteers/Advisors
Mike Watson
Isaac Janak

Leveraging VA Assets to Drive Economic Development

Barry Horowitz – Chair
Maurice Jones
Jandria Alexander
SEC John Harvey

Volunteers/Advisors
David Burhop
Mark Engels

Public Awareness and Culture

Jennifer Bisceglie – Chair
Rhonda Eldridge
SEC Karen Jackson

Volunteers/Advisors
Charlotte Baker, Steven Bucci, Melissa McRae
Capt. Steve Lambert, Don Davidson

Education and Workforce

Andrew Turner – Chair
Richard Clarke
SEC Anne Holton

Volunteers/Advisors
Karen Evans, Diane Miller
Linus Barloon

Cyber Crime

Paul Tiao – Chair
SEC Brian Moran
John Wood

Volunteers/Advisors
Capt. Kirk Marlowe, Linda Bryant, Gene Fishel
Betsi McGrath, Tim Marsh

Key Recommendations
Economic Development Working Group

- **ECON-1: Support workforce development.** Complementary to the Education and Economic Development Work Group recommendations, professional education opportunities should be made available to help managers, regulators, and engineers develop new skills related to security of cyber-physical systems. For example, the 4VA University consortium (University of Virginia, Virginia Tech, James Madison University and George Mason University) could establish a professional education program at the University of Virginia that would grant a certificate in cyber security for physical systems. The program could be expanded to include other state institutions as appropriate.

- **ECON-2: Support cross-sector research funding.** The Commonwealth should fund efforts to facilitate and promote collaborative, competitive, integrated cyber security research and development between cyber security and physical system companies and Virginia's universities. Such R&D would include but not be limited to cyber security issues involving manufacturing, automobile automation and UAV's, and in general anything that falls under the growing "Internet of Things (IoT)" domain. These R&D efforts would create new product and service opportunities at the intersection of cyber security, advanced physical systems and higher education in Virginia.

- **ECON-3: Encourage new company formation.** MACH 37, the Commonwealth's cyber security accelerator engaged in the formation of new cyber security companies, should augment its existing program by adding opportunities focused on the security of physical systems.

- **ECON-4: Leverage Industry Associations to build a cross-industry strategy for advanced manufacturing.** Existing manufacturing and cyber security associations should establish a new integrated work group to develop strategies that will ensure the highest level of security in automated manufacturing. Issues to be addressed include cyber security practices, security certifications for advanced manufacturing companies, threat data sharing, new cyber security technologies and methodologies for joint cyber security technology evaluations.

Key Recommendations
Economic Development Working Group

- **ECON-5: Advanced Automation for Automobile-Specific Initiatives:** Governor McAuliffe in May 2015 announced the formation of a public-private working group to research cyber security in automobiles. The creation of this group not only addresses a high-visibility need but also positions VA as a leader in cyber-physical systems research for automobiles. Initial efforts are already underway to:
- **Develop low-cost technologies** that can be developed to assist law enforcement officers and investigators in determining if/when a vehicle or other mechanized equipment has become the target of a cyber attack.
- **Develop strategies** for Virginia citizens and public safety personnel to identify and prevent cyber security threats targeting vehicles and other consumer devices.
- **Analyze police car vulnerabilities** to cyber attacks and create a cyber security scoring system for vehicles similar to what the Virginia-based Insurance Institute for Highway Safety (http://www.iihs.org/) has for crash worthiness.
- **ECON-6: Unmanned Systems-Specific Initiatives.** Building on the goals of the Commonwealth's Unmanned Systems Commission to bring public and private sector experts together to make recommendations on how to make VA the national leader in unmanned systems by ensuring that such systems are secure from cyber attacks, the Work Group recommended the following:
- **Leverage existing resources** with the National Institute of Standards and Technology and NASA Wallops to develop the cyber security capabilities for unmanned systems that can help create a new industry in VA.
- **Establish a university-based unmanned systems cyber security Center of Excellence** to support the workforce and technology development needed for this emerging area.
- **Develop an economics-based taxonomy of the unmanned systems industry** to identify the most effective ways to advance the economic development efforts in VA related to the intersection of cyber security and unmanned systems.

Key Recommendations
Cyber Crime Working Group

- **C-1: Allowing authentication of Internet content via affidavit.** During criminal prosecutions, Virginia Code currently requires all parties to call an Internet Service Provider's (ISP) custodian of records as a witness to attest to the authenticity of a record of electronic communications. The Work Group recommends Virginia Code § 19.2-70.3 be amended to allow for the authentication of records by the ISP through the submission of an affidavit, which would alleviate an unnecessary burden on the prosecutor and the ISP authenticating the Internet content.

- **C-2: Establish a burden of proof for computer trespass consistent with other states.** Current law requires that the government prove that computer or network intrusions were committed with "malicious intent," an inordinately high burden to meet. The Work Group recommends Virginia Code § 18.2-152.4 be amended to include an additional standard of intent to match more current standards found around the country. Such legislation should also focus on creating a standard of intent that singles out bad actors committing such acts "without authority" to prevent ensnaring innocent conduct. This change will better protect businesses' and citizen's personal computers and information.

- **C-3: Establishing stricter penalties for computer crimes.** Penalties for computer crimes in Virginia are light compared to those of other states and the federal code, which carries felony-level penalties for cyber crimes and cyber security incidents. Rather than treating serious acts of cyber crime as minor violations, the Work Group recommends that computer crime penalties be reviewed and strengthened to bring them in line with more modern computer crime statutes, indicating the seriousness with which Virginia handles such offenses.

Key Recommendations
Cyber Crime Working Group

- **C-4: Defining and increasing associated penalties for crimes targeting government or 'protected' computers and critical infrastructure systems.** As recent hacks of the Office of Personnel Management and the IRS have shown, government agencies are at risk of cyber attack as are the systems controlling the nation's critical infrastructure. However, there are no additional penalties under current law for unauthorized access to these systems. The Work Group recommends that Virginia follow the framework established within federal law, which levies stronger penalties for attacks against government computers and critical infrastructure systems.

- **C-5: Designate violations of the Computer Crimes Act as Racketeer Influenced and Corrupt Organization (RICO) Act predicate offenses.** Under current law, penalties under RICO do not apply to computer crimes even though experience from law enforcement investigations reveals that most major, organized computer crimes are committed across state lines (and even international borders) and typically involve many individuals committing various acts along the criminal chain. The Work Group recommends Virginia amend its RICO statute to include crimes covered by the Virginia Computer Crimes Act so as to strengthen penalties against organized crime operating in cyberspace.

- **C-6: Requesting additional personnel for the Virginia State Police, High Tech Crimes Division (HTCD).** The Virginia State Police conducts primary cyber security investigations and supports the Commonwealth's 340 law enforcement agencies, committing its scarce, specially trained staff to federal, state and local investigations. As computer crimes increase in number and complexity, current employees are overwhelmed. Compounded by personnel shortages, resource constraints force many cyber crimes to go unaddressed. The Work Group recommends hiring additional HTCD staff to deal with these increasing challenges.

Key Recommendations
Cyber Crime Working Group

- **C-7: Leverage universities to address demand for cyber forensics.** Given a limited supply and high demand for cyber forensic analysis expertise, the Virginia State Police HTCD is unable to keep pace with cases requiring cyber forensics, which is becoming increasingly complex because of encryption, mobile devices and cloud computing. The Work Group recommended leveraging university resources – students and cyber security and cyber forensics laboratories – to address HTCD's needs. Using students for some cyber forensic analysis will not only allow HTCD personnel to focus on key cases but also provide invaluable hands-on experience for students looking to enter the field. Furthermore, university laboratories should be made available and used by HTCD and other law enforcement agencies to update and refresh staff cyber forensics skills.

Key Recommendations
Cyber Infrastructure Working Group

- **CI-1: Build the Joint Cyber Security Operations Center (JCSOC) for the purpose of Information Sharing.** The Work Group recommends the creation of a Joint Cyber Security Operations Center (JCSOC). The purpose of the JCSOC is not to replace existing capabilities but to create a hub from which to coordinate resources and gather and disseminate real time threat and vulnerability information to the appropriate parties. Additionally, given an emergency involving a cyber incident, the JCSOC would be leveraged as a resource by the Virginia Emergency Operations Center (VEOC) to provide oversight and resources for a coordinated incident response. The JCSOC will be a key component in the Commonwealth's Information Sharing and Analysis Organization (ISAO), pursuant to the Governor's announcement in April 2015.

- **CI-2: Accelerate Adoption of Identity and Access Management (IAM) and Encryption.** The Work Group recommends that Virginia, on an expedited basis, ensure all personally identifiable information (PII) held by government agencies within the Commonwealth is encrypted and can only by accessed through multifactor authentication. The Work Group recommends that an Encryption, Identity and Access Management program be created and charged with the establishment of a state strategy and operational roadmap. The Commission recommends that a Task Force, co-led by the Virginia Information Technologies Agency (VITA) and the Department of General Services (DGS), be established to review existing IAM programs within the state and to determine a best way forward in addressing E-IAM for the Commonwealth.

Key Recommendations
Cyber Infrastructure Working Group

- **CI-3: Accelerate Adoption of a Common Cyber Security Guidance Framework.** The Commonwealth will continue to pursue the adoption of the Federal Government's National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. VITA, on an annual basis, should evaluate the maturity level of state agencies cyber security programs and practices by leveraging the Framework as a means of assessment.

- **CI-4: Create a voluntary cyber security professional register and the Virginia Cyber Corps to assist local jurisdictions and school districts.** Virginia has a significant cadre of cyber security experts supporting private sector and government programs. However, many small companies, local jurisdictions and school districts are unable to tap such resources. In order to draw additional cyber experts to the Commonwealth and allow companies and jurisdictions to easily identify experts, the Work Group recommends the Commonwealth establish a voluntary register for experts with cyber security credentials to support Virginia's cyber security objectives.

- **CI-5: Leverage the VANG to provide cyber assessment support to Virginia's municipalities.** The Virginia Cyber Security Commission and the VANG have determined that there exists a significant gap in cyber security capabilities in many localities within the Commonwealth. While VITA has developed working relationships with a number of Virginia localities, they do not have the capability to support their information security needs. Through analysis conducted by the Work Group and the VANG, it has been determined that VANG resources can be leveraged by the Commonwealth for the purpose of strengthening the security of locality cyber infrastructure via the assessment of their networks.

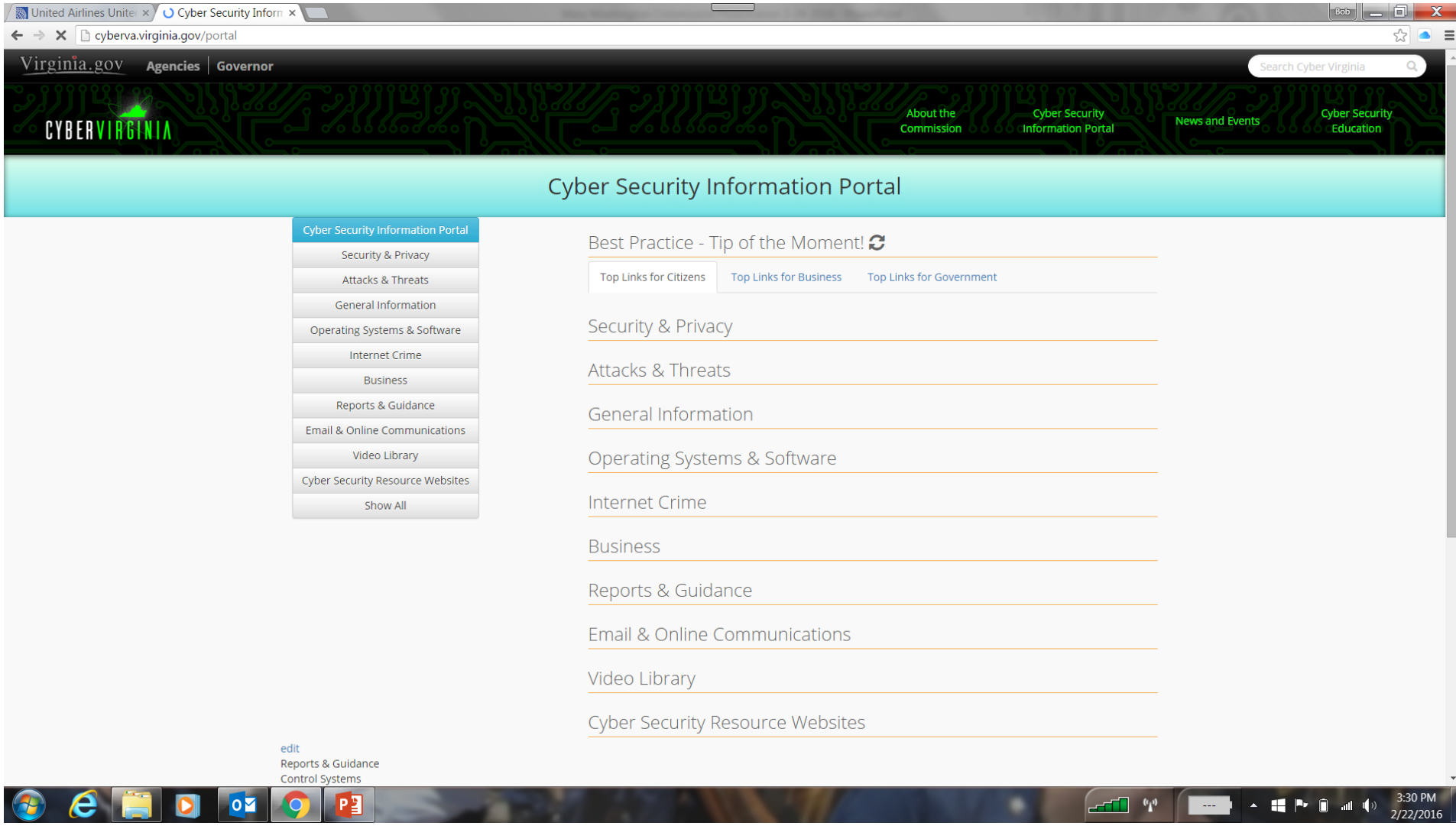
Key Recommendations
Cyber Infrastructure Working Group

- **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.** The security and resilience of critical infrastructure is of the utmost importance to the nation and the Commonwealth. Establishing pilot projects to better secure critical infrastructure serving Virginia installations and bases will not only benefit the military, but also provide added security for other entities that also depend on those services. Much of the infrastructure that is critical to base operations is privately owned and operated. The Office of Public Safety and Homeland Security can provide expertise on matters of critical infrastructure coordination, security, and resilience, and can provide perspective as the Department of Homeland Security's single point of contact for critical infrastructure security and resilience matters.

- **CI-7: Requesting additional personnel for the VFC cyber capability.** The VFC is currently supporting one (1) cyber analyst and one (1) cyber special agent, positions staffed internally from other VFC missions that allow for a limited cyber intelligence capability. As the VFC continues with their cyber mission and looks to further assist in providing expertise in other cyber related initiatives, it will be necessary to establish dedicated cyber resources. For this reason, it is the recommendation of the Work Group that the VFC have additional cyber analyst positions to meet current demands of local, state, and federal entities and to address any future cyber initiatives. This recommendation supports CI-1 through the provision for VFC resources to support the JCSOC's operations.

Key Recommendations
Public Awareness Working Group

- **PA-1: Building a Cyber Information Exchange and Reporting Portal targeted to serve these constituent groups.** A web-based portal with capability to generate out of band alerting to information (text, e-mail, RSS feed, social media) is likely the best mechanism to interface with this broad constituent group. Existing systems like the InnovateVA platform or other Commonwealth web assets could likely be easily adapted for this use. The core resource needed to establish this capability will be the analysts and communications specialist needed to review and extract the pertinent information from the broad amount of data flowing down from federal and other cyber security information feeds. The extracted data will then need to be packaged in such a way that it can be easily consumed and placed in the appropriate communications channel within the portal. Additionally, cyber E911 and 511 like operators should be available to screen reports of cyber incidents and requests for information. Existing Commonwealth call center systems could likely be adapted for these purposes.


United Airlines Unite
Cyber Security Inform
cyberva.virginia.gov/portal
Virginia.gov
Agencies
Governor
Search Cyber Virginia
CYBERVIRGINIA
About the Commission
Cyber Security Information Portal
News and Events
Cyber Security Education
Cyber Security Information Portal
Security & Privacy
Attacks & Threats
General Information
Operating Systems & Software
Internet Crime
Business
Reports & Guidance
Email & Online Communications
Video Library
Cyber Security Resource Websites
Show All
Best Practice - Tip of the Moment!
Top Links for Citizens
Top Links for Business
Top Links for Government
Security & Privacy
Attacks & Threats
General Information
Operating Systems & Software
Internet Crime
Business
Reports & Guidance
Email & Online Communications
Video Library
Cyber Security Resource Websites
edit
Reports & Guidance
Control Systems
3:30 PM
2/22/2016

Key Recommendations
Education and Workforce Development Working Group

- **ED-1: Extend Northern Virginia Community College (NVCC) Program.** At the community college level, the availability of certified cyber security training should be increased in 2017-18 by offering the existing Northern Virginia Community College program to students at any community college in the Commonwealth through distance learning and teleconferencing of the NVCC classes to other campuses and by augmenting faculty (including Adjunct Faculty) at NVCC and other community colleges. The Secretary of Technology and Secretary of Education will begin to develop this initiative in FY2016, working with Northern Virginia Community College and other interested community colleges.

- **ED-2: Obtain Certification for Additional Community Colleges.** In 2017-18, gain certification of three to five additional community colleges by providing supplemental funding for faculty and other elements necessary for the schools to become Academic Centers of Excellence for Cyber Security Education.

- **ED-3: Expand the number of Public Universities certified as Academic Centers of Excellence in Cyber Security Education**. Several of the larger state affiliated universities now offering computer science education, should obtain certification as centers of excellence for cyber security training and gain qualification so that their students can apply for the federal Scholarship for Service funding. Public universities we recommend should achieve this status in the next two years are the University of Virginia, Virginia Tech, Virginia Commonwealth University, and Old Dominion University.

Key Recommendations
Education and Workforce Development Working Group

- **ED-4: Create a Commonwealth Scholarship for Service cyber security program to parallel the National Science Foundation's CyberCorps: Scholarship for Service.** Beginning in FY2017-18 and expanding in the following year, offer state funded scholarships to students who a) obtain their degrees in cyber security at programs in Virginia public universities qualified under the federal Scholarship for Service program and b) commit to working on cyber security in a Commonwealth agency on the same terms as in the federal program.

- **ED-5: Develop a Student Outreach Program for Cyber Security Education.** The Commonwealth should have an active outreach program to inform students and potential students about Commonwealth cyber education programs and the lucrative job openings for trained graduates. The program should specifically target a) active duty military personnel and recently separated veterans, b) high school students in their junior/senior years, c) freshman in VA public colleges/universities.

- **ED-6: Create a shared, virtual Cyber Range for training purposes for students in certified cyber security programs at Virginia public colleges and universities.** Students in cyber security programs need to be able to constructively test their learned abilities in a controlled and safe environment. The Commonwealth can achieve economies of scale by creating a single VA Cyber Range, shared among the public colleges and universities having federally accredited cyber security education programs. The Secretaries of Technology and Education, will conduct a Cyber Range Requirements Study and issue a Request for Information (RFI) in FY2016 to initiate the creation of the Cyber Range.

Key Recommendations
Education and Workforce Development Working Group

- **ED-7: Create the Virginia Cyber Security Education Forum and host Inaugural Cyber Security Education Conference:** This forum would serve as a coordination and information sharing point for the exchange of information among educators and other concerned parties working on cyber security education and training. This Forum would provide input for the Commission's further work in this area and help focus on developing both immediate "quick win" ideas and longer term projects to increase the number and quality of personnel in Virginia's Cyber Work Force.

- **ED-8: Expand Cyber Educational Opportunities and Experiences for Virginia Teachers and Guidance Counselors.** Teachers and guidance counselors are influential in student career choices. Having teachers and counselors trained in cyber security will help foster interest in cyber careers. Additional work is needed to develop a viable plan to achieve this objective.

Follow Cyber Commission and Work Group Activities

http://cyberva.virginia.gov/

View The Full Commission Report

http://cyberva.virginia.gov/media/4396/cyber-commission-report-final.pdf

Questions?