Commonwealth of Virginia Cyber Security Commission

First Report, August 2015

"Threats and Opportunities"

Table of Contents

Transmittal Memo

To: Governor McAuliffe

From: Richard Clarke, Co-Chair Virginia Cyber Commission
Karen Jackson, Co-Chair, Virginia Cyber Commission

Subject: 2015 Report of the Cyber Security Commission

The organizations that created the Internet four decades ago, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation, are located here in Virginia. Since its creation, Virginia has been a focal point for the Internet and associated industries, with the majority of the Internet's traffic passing through its geographical borders. Today, the Commonwealth is home to the most cyber security companies of any state east of the Rockies. Thousands of Virginians work on cyber security every day in corporations, universities, the military, the intelligence community, and in Commonwealth agencies. Thus, we are well positioned to fulfill your intent to make Virginia the Cyber Commonwealth, a state that turns the cyber threat into an engine of growth, prosperity, and security.

The cyber security problem in Virginia, across America, and internationally is acute. Foreign governments and criminal enterprises are engaging in illegal hacking on a massive scale, stealing billions of dollars, committing widespread espionage against governments and corporations, stealing citizens' identities, and threatening to disrupt or destroy networks that are essential to our economy, national security, and way of life. Your goal of maximizing Virginia's potential contribution to cyber security could not have come at a more appropriate time.

The Cyber Security Commission, which you created within weeks of your coming into office, has worked with you, your Executive Team, and the General Assembly to advance that goal. In the last year, Virginia:

- 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 the 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

- Held five Governor's Cyber Security Commission Town Halls, in Blacksburg, Martinsville, Harrisonburg, Charlottesville, and Norfolk to explain the work of the Commission to concerned citizens and benefit from their suggestions and input.

There is, however, much more to be done.

Therefore, we hereby transmit to you twenty-nine specific recommendations to expand Virginia's cyber leadership by improving educational opportunities, increasing cyber related jobs through initiatives focused on new areas of manufacturing and automation, enhancing security of Virginia's critical infrastructure (private and public), making government more effective in achieving its own cyber security, strengthening Virginia's laws against cyber crime, and increasing public awareness and availability of resources related to cyber security.

We look forward to working with you, the Executive Team, and the General Assembly in developing these recommendations into action items for implementation in the near term.

The Commission has also identified in this report, areas for additional work in the next year of its term.

Few issues are more fundamental to the security and prosperity of the Commonwealth and its citizens than the safe, reliable, and secure operation of our computer networks and the systems they enable. On behalf of all the Members of the Commission, we express our thanks for the opportunity you have given us to work with you on this important issue.

Commission Recommendations and Objectives

- Education and Workforce
- Economic Development
- Cyber Crime
- Cyber Infrastructure and Commonwealth Network Protection
- Public Awareness

1. Education and Workforce

Current State

The United States has an acute shortage of trained and certified cyber security professionals. The result is three fold: a) there are tens of thousands of IT security job vacancies in high-paying positions, b) there are far too many personnel performing Chief Information Security Officer roles, or the functional equivalent, throughout the country, who lack the training to do their jobs effectively, and c) as a result, most of the nation's computer networks are more vulnerable to malicious activity, unauthorized entry, data theft, and disruption.

The shortage of cyber security personnel is particularly severe in the Commonwealth, where thousands of good jobs remain vacant. Without a larger pool of cyber security professionals, Virginia will be unable to expand the number and size of cyber security and information technology corporations to its full potential. Without more cyber security experts, the Commonwealth will be unable to protect its own computer networks or the state's critical infrastructure.

Thus, the Commission's highest priority recommendations focus on expanding our Cyber Work Force by creating the nation's largest network of colleges and universities graduating trained cyber security experts from nationally certified higher education programs.

These recommendations include expanding programs at community colleges and graduate degree granting universities. The proposed programs will create more faculty, provide more scholarships, extend outreach to veterans, and add programs at campuses throughout the Commonwealth. Within a few years, these efforts will result in thousands of well-trained cyber security experts entering the Virginia cyber workforce.

Cyber security educational programs at colleges and universities throughout the country are certified by the federal government, based on the recommendations of leading cyber security educators and professionals. There are three relevant programs:

- Centers of Excellence for Education in cyber security https://www.nsa.gov/ia/academic_outreach/nat_cae/
- Centers of Excellence for Research in cyber security https://www.nsa.gov/ia/academic_outreach/nat_cae/
- Scholarship for Service at eligible colleges and universities, where cyber security students can receive federal financial assistance http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228&org=NSF&from=fund

Currently, most of Virginia's public universities offer cyber security courses, but only five of the fifteen public universities are certified by the federal government program for cyber security education through the Academic Centers of Excellence program. A fifth university is certified in cyber research. Only one of the twenty-three community colleges is certified.

Currently six universities, including two private and four state affiliated schools, and one community college in Virginia are part of these federal programs.

Virginia Schools Certified in Federal Cyber Programs

George Mason University	AE[1]
James Madison University	AE, SFS[2]
Norfolk State University	AE, SFS
Virginia Tech University	R[3], SFS
Northern Virginia Community College	AE
Hampton University *	AE, SFS
Marymount University *	AE, SFS
Longwood University	CDFAE[4]

* Private universities

Recommendations

The Work Group recommends that the number of students that are graduating from certified cyber programs in Virginia and the number of such programs in the Commonwealth both be significantly increased. Specifically:

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. Among those 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.

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.

[1] AE schools are certified for educational excellence in cyber security

[2] SFS schools have been certified for their students to receive federal scholarships for service in the federal government following their graduation

[3] R schools are certified for research excellence in cyber security

[4] CDFAE schools have earned the designation of a National Center for Digital Forensics Academic Excellence

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 the cyber security education programs in the Commonwealth and the lucrative job openings for trained graduates. The outreach program should specifically target a) active duty military personnel and recently separated veterans, b) high school students in their junior and senior years, and c) freshman in Virginia public colleges and 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 apply and test their learned abilities (such as network attack and defense) in a controlled and safe environment. The Commonwealth can achieve economies of scale by creating a single Virginia Cyber Range, shared among the public colleges and universities which have federally accredited cyber security education programs.

The Secretary of Technology, in conjunction with the Secretary of Education, will conduct a Cyber Range Requirements Study and issue a Request for Information (RFI) in FY2016 to initiate the creation of the Cyber Commonwealth Range.

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.

Areas for Further Work

The Education Work Group has also considered additional proposals that require its further review in the next year, including:

- Virtual Cyber Dorm: This proposal would create a program for encouraging students at Virginia public colleges and universities to cooperate across disciplines and campuses to develop start-up companies and other enterprises in the area of cyber security.
- Classroom Module for Secondary Schools: This idea would make available to all public secondary schools a grade appropriate teaching package on cyber security to stimulate interest in the field among high school students.
- Virginia Eminent Cyber Educator Recruitment Program: Building on the existing Eminent Researcher Recruitment Program, this proposal would create several Eminent Virginia Cyber Educator positions. These professors would "teach the teachers" at Virginia colleges and universities, tour campuses providing guest lectures, and conduct distance learning classes available throughout the Commonwealth.
- Commonwealth Cyber Corps: The Corps would consist of volunteer experts in cyber security from Virginia's corporations and government agencies who could be certified to serve as Adjunct Faculty at the state's community colleges and universities. The Corps could also sponsor an Industry-Government Exchange Program to permit cyber experts from the private sector to work for a time in the Commonwealth government, and vice versa, sharing their expertise.

2. Economic Development

Current State

The Economic Development Work Group recognizes two national trends that will create additional needs in cybersecurity focused on cyber-physical systems:

1. Rapidly growing initiatives in advanced automation of physical systems (e.g., UAS' automated control of automobiles, digital factories, 3D printers, "Internet of Things")

2. Trend #2 – Cyber attacks have been growing in frequency and sophistication, which can cause physical and economic harm to existing kinetic systems.

Coupled with these trends is the knowledge gap between engineers who design and develop physical systems and the IT professionals who address cyber security. Dual knowledge will be a necessity for securing physical systems and it is in very short supply at this time. In order to adequately address the security concerns for these systems, security must be built in from the beginning through inherently secure design. This creates an opportunity for Virginia businesses and universities to invest in research in these areas of growth in our economy.

A key element of the proposed economic development strategy is to capitalize on existing capabilities and relationships that will provide advantage to Virginia-based companies in responding to the emergent market. These include:

- Knowledge about cyber attacks and defenses residing within our companies supporting our defense and intelligence agencies
- Virginia's trade associations in Cybersecurity and Manufacturing that can help bring together the physical systems and cybersecurity communities
- Existing ties and geographic proximity to the Department of Defense (DoD), the Defense Information Systems Agency (DISA), the Department of Transportation (DOT), the Federal Bureau of Investigation (FBI), the General Services Administration (GSA), and the Department of Homeland Security (DHS)
- Center for Innovative Technology (CIT) GAP/Mach 37 Programs supporting early stage cyber security companies
- Industrial ties to federal government and funded research and development
- Past research and development efforts in unmanned systems, including cyber security research, and other software controlled physical systems such as 3D printers and automobiles
- Virginia-based Federally Funded Research and Development Centers (FFRDC) ,e.g. Mitre, The Aerospace Corporation, Institute for Defense Analysis (IDA); research consortiums, e.g. the Commonwealth Center for Advanced Manufacturing (CCAM) and the Commonwealth Center for Advanced Logistics Systems (CCALS); government research organizations , e.g. the National Aeronautics and Space Administration (NASA); and the Virginia Cyber Security Partnership

Recommendations

The Economic Development Work Group recommends initiatives focused on three areas of economic growth related to cyber security of physical systems including:

- Advanced manufacturing systems

- Advanced automation in automobiles
- Unmanned systems

The Economic Development Work Group formed private-public groups to address each of these areas. The resulting recommendation is to incentivize the cyber security community, higher education community, and the manufacturing/automobile/unmanned systems communities to collaborate and build relationships that will be the basis for leadership in addressing cyber security for physical systems. These collaborations will include joint research efforts, professional education certificate programs, and special industry association programs.

It is recommended that initial steps focus on research, venture capital investment and professional education-related initiatives. Financial resources can be integrated into a fund similar to the Commonwealth's Opportunity Fund that can be holistically managed by a Commonwealth agency or organization. This Work Group recommends focusing on the following initiatives:

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.

ECON-5: Advanced Automation for Automobile-Specific Initiatives: As a result of recommendations made by the Virginia Cyber Security Commission, 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 Virginia 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 Virginia the national leader in unmanned systems by ensuring that such systems are secure from cyber attacks, the Work Group recommends 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 Virginia.
- **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 Virginia related to the intersection of cyber security and unmanned systems.

Areas for Future Work

The Economic Development Work Group will continue to collaborate with and assist the three public-private groups formed during 2014-2015 and will develop specific recommendations for consideration by the full Commission. In addition to continuing support for collaborative research efforts, there will be new and growing opportunities to co-fund research with federal government organizations regarding the unmanned systems and automobile initiatives, enabling Virginia organizations to both contribute and gain recognition for these contributions at the national level. It is expected that, as a result of the funded research efforts resulting from the prior year Commission recommendations, larger companies will be starting to move relevant parts of their cyber security workforce to Virginia and the Commission will play a role in making such opportunities occur.

3. Cyber Crime

Current State

The Cyber Crime Work Group reviewed existing statutes governing crimes in cyberspace including the types of criminal activity covered and the associated penalties. Additionally, the Group focused on improving coordination between the private sector and law enforcement on information sharing and prosecuting cyber crimes.

The Work Group began by conducting a gap analysis of existing Virginia statutes. Among the specific statutes the Work Group reviewed are the Computer Crimes Act, the Child Exploitation Act, and the Data Breach Notification Act. Key assistance was provided by students from The George Washington University's Trachtenberg School of Public Policy, who conducted significant research and analysis to compare Virginia laws to those of other states and federal law. The students worked with members of the Commission, the Virginia Attorney General's office, Virginia State Police, and the Office of Public Safety and Homeland Security. As a result of the group's research, the Work Group proposed, introduced (and successfully passed in the 2015 General Assembly session) legislation to support law enforcement in its

fight against cyber crime and to protect the public by preventing the release of information that would jeopardize the safety or the security of citizens, facilities and information systems. Commission sponsored legislation included:

Sealing of administrative subpoenas for electronic communications and social networking data (SB919/HB1946). Under recommendation from the Virginia Cyber Security Commission and with bipartisan support, the General Assembly passed SB919/HB1946 to help protect Virginia children from online exploitation and to allow law enforcement to effectively investigate crimes involving child pornography, child exploitation, and human trafficking. The bills ensure that child predators are not informed of ongoing investigations and will help law enforcement quickly remove children from dangerous exploitative situations.

Passage of these bills represents important progress in the fight against cyber criminals and online predators. The bills allow for a prosecutor to seal a subpoena seeking the identity of someone who has produced, distributed, or downloaded child pornography. This will ensure that criminals will not be tipped off and attempt to destroy evidence or flee prosecution. The bills also allow prosecutors to find out the identity of someone posting online advertisements for sexual encounters with children or victims of human trafficking. Such requests have been available to prosecutors and investigators since 2007, but by keeping such requests under seal for 30 days, prosecutors and investigators can more effectively identify and investigate these predators and criminals.

Clarifying language for search warrants surrounding the seizure and examination of computers, networks, and other electronic devices. The Commission also recognized the need to clarify language surrounding what may be searched and seized as it pertains to digital media. The General Assembly passed SB1307 that amends § 19.2-53, which governs what may be searched and seized. As was the Cyber Security Commission's intention, this law addresses the evolution of technology and the need to amend outdated legislation with regards to cyber security. Prior to the passage of SB1307, the law did not specify whether or not the initial search warrant, which authorizes the lawful seizure of digital evidence, allowed law enforcement to collect such evidence from the piece of media away from the initial scene. The bill provides that any search, including the search of any computer, computer network, or other device, may be conducted in any location and not just the location where the evidence was seized. SB1307 also amends § 19.2-53 to include the physical components or electronic or digital information of any computer, computer network, or other device. The Commission emphasizes that this bill in no way increases the authority of law enforcement or the scope of the search and seizure and believes that this legislation will go a long way in providing much needed support for law enforcement in the ever evolving fight against cyber crime.

Securing FOIA exemptions for sensitive information regarding cybersecurity threats and vulnerabilities (SB1109 and SB1129). The Freedom of Information Act (FOIA) affords all citizens of the Commonwealth the ability to request access to government records and meetings. However, to protect the public, certain sensitive information regarding public safety and homeland security must be kept private. One of the Cyber Security Commission's priorities was to make sensitive cyber security information exempt from FOIA requirements. Influenced by the Cyber Security Commission, SB1109 and SB1129 were introduced and successfully passed to protect this kind of information. SB1109 expands the open meeting exemption for the discussion of plans to protect public safety as it relates to terrorism and security of governmental facilities to include the discussion of specific cyber security threats or vulnerabilities. Similarly, SB1129 applies to FOIA exemptions for records containing cyber security threat and vulnerability information. Both bills are intended to protect the public by preventing the releasing of information that would jeopardize the safety of any person or the security of any facility, building, structure, information technology system, or software program.

Recommendations

As crimes move from the physical world into cyberspace, the Work Group focused its research on ensuring that Virginia's laws must be updated to address the latest technologies and aligned with statutes in other states. The Work Group's legislative recommendations for conducting more effective cyber security investigations and bringing successful prosecutions include:

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.

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.

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 recommends 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.

Areas for Future Work

The Work Group contends that the proposed recommendations will greatly improve Virginia's ability to investigate and prosecute cyber criminals. If enacted, the Commonwealth will be moving in the right direction to better enable Virginia's law enforcement to investigate cases of cyber crime; however, much more work must be done. Areas where the Work Group may further investigate include, but are not limited to:

- Evaluating the lawful use of technology by law enforcement for crime fighting applications, considering impacts to public safety and privacy
- Increasing awareness of the types of cyber threats and the risks they pose to the public, a subject which will require collaboration with the Public Awareness Work Group
- Identifying opportunities for training and collaboration among state agencies, specifically focusing on cyber criminal investigations and forensics
- Examining the increased emphasis on mobile devices, both within and outside of the workplace, and their potential impacts on cyber crime and privacy
- Investigating the feasibility of improving Virginia's laws and regulations governing cyber crime, specifically on the issue of the trafficking of passwords
- Investigate protections and policies around ethical hacking and its legitimate use in cyber defense strategies
- Explore the uses of encrypted communications and severity of the impact it has on investigating cyber crime when used by criminals

4. Cyber Infrastructure and Commonwealth Network Protection

Current State

The current Commonwealth information technology infrastructure consists of an enterprise network with data connections located throughout Virginia. It includes: over 60,000 workstations, over 3,000 servers, more than 1.5 petabytes of data, and thousands of phones and mobile devices. The Virginia Information Technologies Agency (VITA) is responsible for providing both information technology (IT) oversight, in the form of governance to Commonwealth agencies, and infrastructure services to executive branch agencies.

Individual agencies remain responsible for the applications needed to support their business operations. One of VITA's primary responsibilities includes strategic and operational oversight for cyber security in the Commonwealth. VITA remains the primary agency responsible for detection and response across most Commonwealth networks, but is limited in authority over the entire Commonwealth infrastructure because of the distributed nature of authorities and responsibilities associated with agency applications.

In addition to having an understanding of how IT and IT security is managed in Virginia, the Cyber Infrastructure and Commonwealth Networks Protection Work Group developed an understanding of capabilities that exist in the state surrounding cyber security. The Work Group focused its key engagements and discussions with the following organizations over the course of the past year.

Virginia Information Technologies Agency (VITA) is the Commonwealth's consolidated information technology organization. Responsibilities fall into four primary categories:

- Governance of the Commonwealth's information security programs in support of the responsibilities of the Chief Information Officer of the Commonwealth
- Operation of the IT infrastructure, including all related personnel, for the executive branch agencies declared by the legislature to be "in-scope" to VITA
- Governance of IT investments in support of the duties and responsibilities of the Information Technology Advisory Council and the Chief Information Officer of the Commonwealth
- Procurement of technology for VITA and on behalf of other state agencies and institutions of higher education

The Virginia National Guard (VANG) has the largest single cyber capability in the entire National Guard. VANG personnel are currently assigned to various U.S. Cyber Command teams that provide a broad range of cyber security capabilities towards defending various DoD networks and systems. The VANG also facilitates Virginia's Cyber Response Work Group. This Work Group is made of representatives from 7 State/Localities, 4 Federal Agencies, and the Governor's Office. Since 2011, the VANG has participated in National Level Cyber Exercises such as the U.S. Cyber Command's Cyber Guard (focus on protection of critical infrastructure), DoD's Cyber Flag (focus on federal cyber National Mission Forces), and the National Guard's annual Cyber Shield exercise (focus on defense of military networks).

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.

Virginia State Police – 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. 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

The Virginia Cyber Security Partnership is a collaboration of public and private organizations within Central Virginia to include federal and state agencies, as well as critical infrastructure companies, e.g. finance and energy sectors. Its focus is on the mutual sharing of information and intelligence involving cyber threats and malicious actors

While these targeted engagements provided valuable insights into the existing capabilities of Virginia's cyber security programs, the Work Group also undertook the following activities to further understand the Commonwealth's position:

- A survey of the overall cyber security posture of all Virginia agencies. The survey responses have been provided to Virginia Commonwealth University for analysis, development of key findings and initial recommendations.
- Assessment of the cyber capabilities of the Virginia National Guard and its ability to provide support for evaluating and enhancing cyber readiness of Virginia municipalities.
- Review of the cyber security processes and procedures being used to protect personally identifiable information (PII) at five Virginia agencies holding large amounts of citizen data.

Recommendations

Though the Work Group expects additional recommendations after the final analyses of the surveys of agency systems and PII protection processes are complete, the initial recommendations generated from the Work Group activities include:

CI-1: Build the Joint Cyber Security Operations Center (JCSOC) for the purpose of Information Sharing. The Commonwealth has several organizations that exchange cyber security related information but there is no common means of analyzing and disseminating cyber specific data. For example, the VITA's ability to monitor critical agency networks is not well connected with the VFC or the VANG. Other partnerships such as the Virginia Cyber Security Partnership are not able to connect easily and share. In order to establish a fluid means of exchange relevant cyber vulnerability and incident among Virginia agencies, partners, and critical infrastructure operators, 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 leverage a small team of security operators and technologies to securely exchange data and foster collaboration. 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 recent trends in high profile data breaches demonstrate that identity and access management, and properly implemented encryption have major benefits for many network environments. 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.

In order to execute this initiative, 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. The Task Force should also determine a single agency to be charged with establishing and managing an E-IAM program for the Commonwealth. Agencies represented on this Task Force should include, but are not limited to, the Virginia Department of Emergency Management (VDEM), the Virginia State Police (VSP), the Virginia Department of Motor Vehicles (DMV), the Virginia Department of Transportation (VDOT), and the Virginia Department of Health (VDH).

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. The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cyber security risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cyber security management communications amongst both internal and external organizational stakeholders. 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 that results in a vetted roster of personnel with appropriate skills to support Virginia's cyber security objectives.

Furthermore, the Commonwealth has many local jurisdictions and school districts that need help assessing the security of their networks. Their budgets are tight and many do not have the staff address critical cyber security challenges. As a means to ensure cyber security is addressed across the entire Commonwealth in a cost effective manner, the Work Group recommends establishing a Virginia Cyber Corps (VCC). The VCC will be managed by the state but will be staffed by volunteers drawn from the voluntary cyber security professional register. The VCC will establish criteria for local jurisdictions and school districts to request assistance. The VCC will also create a database of those entities requesting assistance. Those experts listed in the professional register may offer their time to local jurisdictions and school districts seeking assistance in return for tax incentives.

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.

The VANG Cyber Commander is capable of committing up to ten (10) personnel for the purpose of supporting state cyber missions. There are two missions which have been identified for support from the VANG. The first is to conduct locality network vulnerability assessments which would consist of a team of two (2) service members, conducting assessments on site at the locality for a period of approximately three (3) days. Upon completion of the assessment, localities would receive a written report of their network vulnerabilities. The second mission would be to perform state agency website vulnerability assessments which would consist of one to two (1-2) soldiers and could be conducted off-

site from the Agency. A single state agency website could be assessed in less than one (1) day, and should not require interaction with the actual state agency.

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.

Areas for Future Work

The Commonwealth of Virginia Agency Cyber Security Survey as well as other briefings and discussions held by the Work Group revealed several opportunities for improved cyber security response as well as improved protections for Virginia government and citizen data. Future areas of interest and investigation by the Cyber Infrastructure and Commonwealth Network Protection Work Group will focus on three broad themes: 1) understanding and responding to the threat; 2) serving Virginia citizens and 3) protecting Commonwealth IT infrastructure assets. Specific work includes, but is not limited to:

- Identifying alternatives for improving the cyber security posture of Virginia's small and medium sized businesses through a combination of governmental, industry, and/or citizen volunteer efforts.
- Providing increased protection recommendations for Commonwealth agencies that provide citizen-services via Internet-based applications or web sites.
- Reviewing current contracting language used by Commonwealth agencies to ensure appropriate and consistent levels of monitoring, reporting, and accountability of third-party, supply chain providers with respect to cyber security vulnerabilities and government and/or citizen data.
- Reviewing Virginia's current policy development and risk monitoring organizational structure to ensure consistent risk evaluation and appropriate cyber security standards are developed and applied to all Virginia governmental and quasi-governmental organizations; consider establishing a centralized office whose authority to establish and update standards appropriate for the risk extends throughout the Commonwealth.
- Explore the current information security environment in localities and, identify gaps, develop recommendations, and prioritize those recommendations to address shortfalls in local information security programs

5. Public Awareness

Current State

Over the last year, the Public Awareness Work Group held Town Hall meetings and participated in public events throughout the Commonwealth, reaching more than 900 citizens to explain the objectives of the Virginia Cyber Security Commission, provide cyber security insight from subject matter experts and, most important, solicit feedback on attendees' cyber security concerns. Additionally this year, the Commission members partnered with other organizations focused on cyber, to reach almost 1,700 citizens.

Based on feedback received during the outreach events, the Public Awareness Work Group found that counties, municipalities, small to mid-sized businesses and citizens need a reliable source of clear, concise and understandable cyber threat information, including best practices and processes for requesting cyber security remediation assistance as well as a way to report suspected cyber incidents.

While there are many information exchanges for federal and state cyber security agencies and large businesses (especially those operating critical infrastructure), the same opportunities do not exist at the regional and local levels. Often, cities and counties often cannot afford the cyber security trained personnel to access threat sharing and remediation resources. Those municipalities with cyber security staff are often challenged to convey the complexity and critical importance of addressing and remediating cyber threats to their leadership. And small and medium sized businesses don't have the resources to assign to this issue. Commonwealth citizens are left to their own.

Recommendations

To address these issues the Work Group recommends:

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.

This concept aligns well with recommendation CI-1 referenced earlier in this document.

Areas for Future Work

The Public Awareness Work Group will continue to refine the requirements, capabilities and resources needed for the Cyber Information Exchange and Reporting Portal. This effort will be closely coordinated with Cyber Infrastructure and Commonwealth Network Protection Work Group activities related to the JCSOC and the Virginia ISAO to ensure an integrated and cost effective approach to gathering, analyzing, and disseminating cyber security information.

Based on the interest generated during the Virginia Cyber Security Commission's first year of cyber security outreach, the Work Group expects to continue conducting Town Hall meetings and other informational events throughout Virginia.

Appendix A

Executive Order 8

Commonwealth of Virginia Office of the Governor

Executive Order

NUMBER EIGHT (2014)

LAUNCHING "CYBER VIRGINIA" AND THE VIRGINIA CYBER SECURITY COMMISSION

Importance of the Issue

The Commonwealth of Virginia is proud of its distinguished history and exemplary record of exceptional cyber security operations in support of state agencies and operations. As is reflected in the strong presence of state, federal, military, and private cyber security businesses, assets, and activities throughout the Commonwealth, Virginia stands poised to take advantage of its unique resources. The Commonwealth is resolute in its dedication to garnering the expertise of leaders in cyber security in order to mitigate risks and safeguard the highest level of security for government infrastructure networks, foster cyber security education and awareness, incorporate innovative and best practices to protect data statewide, bolster business investment with public-private partnerships, and proactively enhance its national standing as one of the preeminent leaders in the cyber security arena.

Threats to critical systems present a growing and complex challenge. In order to guard against the risks and marshal appropriate resources to meet potential threats, it is important to incorporate optimal policies and develop enhanced standards to protect the Commonwealth's cyber security infrastructure from unforeseen incidents. While rapidly advancing technologies create substantial security risks, they also present significant opportunities for producing more efficient and protected proprietary networks, strengthening the Commonwealth's cyber security framework, and advancing vital prospects for economic development.

Virginia's cyber security businesses are at the forefront to prospectively benefit from federally appropriated funds that are among the few expected to increase in future years. Virginia's cyber security firms are seeking to export their technologies, goods and services to global markets in the public and private sectors. Further, with military assets, related defense activities and, more generally, the critical need for secure business data, the Commonwealth must cultivate

conditions to attract and retain as well as secure a competitive advantage for cyber security companies in the marketplace. Promotion of the cyber security industry will produce a synergy to ensure growth of related cyber operations businesses and facilities, sustain a wide variety of high-skilled jobs for Virginians, and strengthen a culture of excellent cyber hygiene that is critical for the Commonwealth.

Cyber security instruction, training, and programs will be requisite components to prepare those currently seeking new occupational options as well as the next generation for the rapidly developing cyber security workplace. Focusing on cutting edge education and training will be essential for Virginia's cyber security workforce and economic development as occupations in the cyber security industry are highly in demand and among the fastest growing in the economy. Virginia continues to lead the nation in the concentration of technology workers, fed by a rich network of nationally-recognized information technology and cyber advanced degree programs at our universities.

Composition of the Commission

The Commission will consist of the Secretaries of Technology, Commerce and Trade, Public Safety, Education, Health and Human Resources, and Veterans Affairs and Homeland Security, and eleven (11) citizen members whose background shall include relevant expertise to be appointed by the Governor and serve at his pleasure. The Governor shall designate a Chairman and Vice Chairman from among the appointed members. The Governor may appoint additional persons to the Commission at his discretion.

Establishment of the Commission

Accordingly, by virtue of the authority vested in me as Governor under Article V of the Constitution of Virginia and under the laws of the Commonwealth, including but not limited to §§ 2.2-134 and 2.2-135 of the Code of Virginia, and subject to my continuing and ultimate authority and responsibility to act in such matters, I hereby establish the Virginia Cyber Security Commission.

Responsibilities of the Commission

Commission's responsibilities shall include the following:

1. Identify high risk cyber security issues facing the Commonwealth of Virginia.

2. Provide advice and recommendations related to securing Virginia's state networks, systems, and data, including interoperability, standardized plans and procedures, and evolving threats and best practices to prevent the unauthorized access, theft, alteration, and destruction of the Commonwealth's data.

3. Provide suggestions for the addition of cyber security to Virginia's Emergency Management and Disaster Response capabilities, including testing cyber security incident response scenarios, recovery and restoration plans, and coordination with the federal government - in consultation with the Virginia Information Technologies Agency.

4. Offer suggestions for promoting awareness of cyber hygiene among the Commonwealth's citizens, businesses and government entities.

5. Present recommendations for cutting edge science, technology, engineering and math (STEM) educational and training programs for all ages, including K-12, community colleges, universities, in order to foster an improved cyber security workforce pipeline and create cyber security professionals with a wide range of expertise.

6. Offer strategies to advance private sector cyber security economic development opportunities, including innovative technologies, research and development, and start-up firms, and maximize public-private partnerships throughout the Commonwealth.

7. Provide suggestions for coordinating the review of and assessing opportunities for cyber security private sector growth as it relates to military facilities and defense activities in Virginia.

Commission Staffing and Funding

Necessary staff support for the Commission's work during its continued existence shall be furnished by the Office of the Secretary of Technology, and such other agencies and offices as designated by the Governor. An estimated 500 hours of staff time will be required to support the work of the Commission.

Necessary funding to support the Commission and its staff shall be provided from federal funds, private funds, and state funds appropriated for the same purposes as the Commission, as authorized by § 2.2-135 of the Code of Virginia, as well as any other private sources of funding that may be identified. Estimated direct costs for this Commission are $5000.00.

Commission members shall serve without compensation and shall receive reimbursement for expenses incurred in the discharge of their official duties.

The Commission shall serve in an advisory role, in accordance with § 2.2-2100 of the Code of Virginia and shall meet upon the call of the chairman at least three times per year. In addition, the Commission shall issue an annual report and any other reports and recommendations as necessary or as requested by the Governor.

Effective Date of the Executive Order

This Executive Order shall be effective upon its signing and shall remain in force and effect until February 25, 2015, unless amended or rescinded by further executive order.

Given under my hand and under the Seal of the Commonwealth of Virginia, this 25th day of February, 2014.

Terence R. McAuliffe, Governor

Attest: _____

Secretary of the Commonwealth

Appendix B

Virginia Cyber Security Commission Members

Commission is co-chaired by Richard Clarke and Secretary of Technology, Karen Jackson.

Richard A. Clarke, Chairman and CEO of Good Harbor Security Risk Management and an internationally recognized expert on cyber security, homeland security, national security, and counterterrorism. Mr. Clarke served the last three presidents as a Senior White House Advisor, including as Special Advisor to the President for Cyber Security and National Coordinator for Security and Counterterrorism, and was a member of President Obama's Review Group on Intelligence and Communication Technologies. He is a member of the Education and Workforce Work Group

Karen Jackson, Secretary of Technology and member of the Public Awareness Work Group.

Anne Holton, Secretary of Education and member of the Education and Workforce Work Group.

John Harvey, Secretary of Veterans and Defense Affairs and member of the Education and Workforce Work Group and the Economic Development Work Group.

Dr. Bill Hazel, Secretary of Health and Human Resources and member of the Infrastructure and Commonwealth Network Protection Work Group.

Maurice Jones, Secretary of Commerce and Trade and member of the Economic Development Work Group.

Brian Moran, Secretary of Public Safety and Homeland Security and member of the Cyber Crime Awareness Work Group.

Rhonda Eldridge, Director of Engineering at Technica Corp. where she leads six divisions within Technica and is responsible for internal research and development, visioning and business development – focusing on cutting edge cyber security and IT projects for federal customers including the Department of Defense. She is a member of the Public Awareness Work Group.

Jennifer Bisceglie, President and CEO of Interos Solutions, Inc. Ms. Bisceglie has more than 20 years of commercial technology and business operations experience in cyber security, business process re-engineering and commercial technology implementation for diverse companies industries and governments. She is chair of the Public Awareness Work Group.

Paul Kurtz, Chief Strategy Officer at CyberPoint. Mr. Kurtz leads the development and communication of CyberPoint's strategic vision for managing cyber threats. A recognized cyber security expert, he has held senior positions in both industry and government. During his government service, Kurtz was Special Assistant to the President and Senior Director for Critical Infrastructure Protection on the White House's Homeland Security Council. He is chair of the Infrastructure and Commonwealth Network Protection Work Group.

Paul Tiao, Attorney and partner with the international law firm of Hunton and Williams, LLP, where he is a leader in the firm's global privacy and cyber security practice. Prior to joining the firm, Mr. Tiao served as Senior Counselor for cyber security and technology to FBI Director Robert S. Mueller. He is chair of the Cyber Crime Awareness Work Group.

Barry Horowitz, Munster Professor of Systems and Information Engineering and Chair of the Systems and Information Engineering Department at the University of Virginia. Dr. Horowitz' research efforts center on economic models and system technologies related to cyber security. He currently is leading a Defense Department-sponsored research effort focused on embedding security solutions into systems, referred to as System Aware Cyber Security. Dr. Horowitz serves as a member of the Naval Studies Board of the National Academy of Science and recently led a Chief of Naval Operations-sponsored study for the board on cyber security. He is chair of the Economic Development Work Group.

Andrew H. Turner, Senior Vice President and Head of Global Security, VISA. Mr. Turner developed, from the ground up, VISA's Cyber Security organization, including the Attack Surface Management, Threat Intelligence, Incident Response and Digital Brand Protection Programs. He also implemented a Cyber Fusion-based program using intelligence collection, analysis and overall sensor enrichment to actively monitor and defend against global threats to the VISA enterprise and ecosystem. Prior to joining VISA, Mr. Turner served as Cyber Intelligence Practice Director for Microsoft Corp. He is chair of the Education and Workforce Work Group.

Jeffrey C. "J.C." Dodson, Global Chief Information Security Officer, BAE Systems. Mr. Dodson is a global cyber security expert across government, defense, aerospace, law enforcement and advanced technology sectors. He is the chairman of the Aerospace Industries Association's Industrial Security Committee and was appointed to serve as an Industry Representative to the federal government's National Industrial Security Program Policy Advisory Committee. He is a member of the Infrastructure and Commonwealth Network Protection Work Group and the Cyber Crime Awareness Work Group.

Jandria Alexander, Principal Director of the Cyber Security Subdivision in the Engineering Technology Group at the Aerospace Company. Ms. Alexander currently leads cyber and network security support to numerous customers and leads teams performing systems engineering for cyber operations, including architecture, requirements and concept of operations (CONOPS) support for integrating cyber operations into advanced ground and space segments. She is a member of the Economic Development Work Group and the Public Awareness Work Group.

Elizabeth "Betsy" Hight, Retired U.S. Navy Rear Admiral who served as the Vice Director of the Defense Intelligence Agency (DISA), Ms. Hight most recently served as Vice President of the Hewlett Packard's Enterprise Services U.S. Public Sector Cybersecurity Practice. She is a member of the Infrastructure and Commonwealth Network Protection Work Group.

John Wood, Chief Executive Officer, Chairman of the Board and Director for Telos Corp. As CEO, he orchestrates the company's support of the federal government in the critical areas of cyber operations and defense, secure communications and collaboration and identity assurance. He is a member of the Cyber Crime Awareness Work Group.

Rear Admiral Bob Day, U.S. Coast Guard (ret), Coast Guard CIO and Cyber Commander 2009-2014. He is the Virginia Cyber Security Commission Executive Director responsible for daily management of Commission activities.

Appendix C

Commission Meetings

The Commission and Work Groups conducted official meetings on the following dates:

June 11, 2014 - Inaugural Meeting
George Mason Inn, George Mason University

September 4, 2014 - Commission Meeting
Richmond Hilton Conference Center, Short Pump

November 7, 2014 - Commission Meeting
Patrick Henry Building, Richmond

March 18, 2015 - Commission Meeting
Patrick Henry Building, Richmond

May 6, 2015 - Commission Meeting
Virginia Tech Research Center, Arlington

July 7, 2015 - Commission Meeting
Patrick Henry Building, Richmond

Additional Work Group meetings were held on numerous dates.

All Commission and Work Group meeting agendas and minutes are available at https://cyberva.virginia.gov/Meeting-Resources.