MARYLAND

Commission on Maryland Cybersecurity Innovation and Excellence

FINAL REPORT
FINDINGS AND RECOMMENDATIONS

September 1, 2014

Executive Summary

The unprecedented increase in number and severity of cyberattacks cost the global economy about $445 billion each year. The identities and bank accounts of hundreds of millions of Americans had been threatened and compromised. There is a critical need for ensuring that our nation has the workforce, technology and resources to protect our citizens, businesses, infrastructure, privacy and intellectual property. Maryland continues to be a leader on this front.

Many of the federal agencies that are focused on this important task are headquartered in Maryland including the US Cyber Command, National Security Agency, the National Institute of Standards and Technology, and the Defense Information Systems Agency. More venture funds are deployed for cybersecurity companies and excellent cyber incubators exist in Maryland offering start-up support for innovation. There are 24 National Centers of Academic Excellence in Information Assurance/Cyber Defense educating and developing cybersecurity workforce of today and the future in Maryland. This provides an ecosystem for cybersecurity innovation and job growth in Maryland. Even though Maryland has these strengths in cybersecurity, there are some gaps that need to be addressed to ensure the protection of critical information infrastructure and further enhance cyber innovation and job creation in the state.

The two main components of the charge of the Commission on Maryland Cybersecurity Innovation and Excellence include: (1) to conduct an overview of current state, federal, and international laws in order to provide recommendations for laws and/or policies; and (2) to provide a strategic roadmap for making Maryland the leader in cybersecurity innovation and job creation. To achieve these two main components, the Commission focused on four main themes: legal strategy, state structure and practice, marketing and partnerships, and education and training. The Commission’s findings and recommendations organized around these four main themes will significantly help the State in becoming the epicenter of cybersecurity innovation and excellence.

The Commission has been successful in supporting efforts contributing to the passage of legislation aimed at protecting the critical information infrastructure; enhancing cybersecurity awareness; and formulating strategic recommendations for making Maryland the leader in cybersecurity innovation and job creation. To increase cybersecurity awareness among the state legislators, leaders of public and private sector organizations and general public in Maryland, the Commission has conducted regular meetings, open receptions during the General Assembly sessions, a briefing to an international delegation, and cybersecurity awareness events. The Commission commends the passing of two major pieces of first ever legislation to protect sensitive data held by state agencies against cyber attacks and to protect health care records from identity theft. The second law is particularly timely as our state moves toward electronic health care records.

The Commission is committed to making further progress and in continuing to assist in protecting our state government, economy, and infrastructures from cyber attacks and developing strategies for promoting innovation, technology transfer, and pipelines for cyber jobs at all levels. To continue its critical work, the Commission recommends the extension of the Commission’s term beyond 2014.

Table of Contents

I. Background & Introduction

The Commission on Maryland Cybersecurity Innovation and Excellence was created when Governor Martin O'Malley signed House Bill 665 on May 10, 2011. The establishment of the Commission is codified in Md. Code Ann. State Gov't § 9-2901 (2011). In accordance with that statute, the "purpose of the Commission is to provide a road map for making the State the epicenter of cybersecurity innovation and excellence." Md. Code Ann. State Gov't § 9-2901(f) (2011).

The Commission on Maryland Cybersecurity Innovation and Excellence, which is composed of representatives of large and small companies, academia, state and federal agencies, and nonprofit organizations, is tasked with providing legislative and policy recommendations for protecting our state government, economy, and infrastructures from devastating cyber attacks and producing strategies for developing and promoting innovation, technology transfer, and pipelines for cyber jobs at all levels.

II. Commission Membership

- Susan Lee, Co-Chair, Delegate, Maryland House of Delegates
- Catherine Pugh, Co-Chair, Senator, Maryland Senate
- Russell Butler, Executive Director/Attorney, Maryland Crime Victims' Resource Center, Inc.
- Chieh-San Cheng, President and CEO, Global Science & Technology, Inc.
- Darrell Durst, Vice President, Lockheed Martin
- Sean Fahey, Research and Development Program Manager, John Hopkins University Applied Physics Laboratory
- Frederick Ferrer, Chief, Critical Infrastructure/Key Resources Branch, Anti-Terrorism Division, Maryland Coordination and Analysis Center
- Derek Gabbard, Founder & CEO Lookingglass Cyber Solutions, LLC
- Rick Geritz, CyberHive LLC
- Barbara Gonzalez, Manager - Special Projects, NERC, Pepco Holdings, Inc.
- Samuel J. Gordy, Group President, Integrated Systems Group, Leidos
- Michael Greenberger, Law School Professor & Director, University of Maryland Center for Health & Homeland Security
- Rear Admiral Elizabeth (Betsy) A. Hight (USN, Ret.), Former Vice President, U.S. Public Sector Cybersecurity Practice, HP Enterprise Services
- Clay House, Vice President Architecture, Planning, and Security Carefirst BCBS
- Leonard J. Howie III, Secretary of the Department of Labor, Licensing, and Regulation
- Joe Jarzombek, Director, Software & Supply Chain Assurance, U.S. Department of Homeland Security Office of Cybersecurity and Communications
- Belkis Leong-Hong, Founder, President & CEO Knowledge Advantage Inc.
- Larry Letow, TCM Chairman and President and COO, Tech Council of Maryland
- Terry Lin, CEO, Planned Systems International, Inc.
- Katherine Michaelian, Instructional Dean, Montgomery College

- Dominick Murray, Secretary of Business and Economic Development
- Robert A. Rosenbaum, Executive Director, Maryland Technology Development Corporation
- Elliot H. Schlanger, Director of Security and Chief Information Security Officer, State of Maryland, Department of Information Technology
- Deon W. Viergutz, President, Fort Meade Alliance
- David Wilson, President, Morgan State University

III. UMUC's Role

The role of University of Maryland University College (UMUC) is to assist the Commission on Maryland Cybersecurity Innovation and Excellence in planning and hosting Commission meetings, open receptions during General Assembly sessions and cybersecurity awareness events; bringing expert resources to support the Commission's work; working with the Commission members and their institutions to support the Commission's efforts; and drafting commission reports. In addition, UMUC hosts and maintains the Commission's website at: http://www.umuc.edu/legal/cyber/. The Commission is being staffed by the UMUC's representative, Dr. Amjad Ali, Associate Vice President and Cybersecurity Advisor to the President. The Commission also acknowledges the work of Dr. Greg von Lehmen, former UMUC's Senior Vice President of External Relations and Initiatives in staffing the commission from November 2011-June 2013.

IV. Commission Structure

The two main components of the Commission's charge include: (1) to conduct an overview of current state, federal, and international laws in order to provide proposed recommendations for laws and/or policies; and (2) to provide a strategic roadmap for making Maryland the leader in cybersecurity innovation and job creation. To achieve these two main components, the Commission is organized into an executive committee and subcommittees around the four major themes: legal strategy, state structure and practice, marketing and partnerships, and education and training.

Executive Committee

The role of the executive committee is to receive periodic updates from Subcommittee Chairs and to provide feedback and direction to the Chairs of the Commission's subcommittees. The executive committee includes the following:

- Susan Lee, Co-Chair, Delegate, Maryland House of Delegates
- Catherine Pugh, Co-Chair, Senator, Maryland Senate
- Chairs of the Commission's Subcommittees

Commission Subcommittees

The following are the Commission's Subcommittees organized around the four major themes: legal strategy, state structure and practice, marketing and partnerships, and education and training:

Subcommittee on Legal Strategy

The Legal Strategy Subcommittee is charged with:

- Conducting a comprehensive review of and identifying inconsistencies in:
  - State and Federal cyber security laws
  - Policies, standards, and practices for ensuring security of:
    - Educational institutions,
    - State government, and
    - Other organizations working with health, personal identification, public safety, public service, and utilities information
- Identifying any federal preemption issues relating to cyber security methods state can use to increase cyber innovation
- protecting intellectual properties
- Recommending legislation and policies to increase cyber innovation in the state

The members of Legal Strategy Subcommittee are:

- Michael Greenberger, Subcommittee Chair, Law School Professor & Director, University of Maryland Center for Health & Homeland Security
- Russell Butler, Executive Director/Attorney, Maryland Crime Victims' Resource Center, Inc.

The findings and recommendations of the Subcommittee on Legal Strategy are included in Appendix.

Subcommittee on State Structure and Best Practices

The Subcommittee reviewed the many resources, programs, best practices, and opportunities that already exist and are evolving in Maryland and the US Federal Government that might be leveraged by the Department of Information Technology (DoIT), State agencies, and those operating Maryland's critical infrastructure upon which citizens rely for services. The Subcommittee deliberated on state-level security topics for the following consideration:

- Security vs. Compliance, how much should organizations deal with compliance, if at all?
- To what State function should a State CISO report?

- Policy and enforcement vs. guideline and support vs. hybrid approach:
    - Hybrid Option for "guide" until state organization "proves" help is needed (based upon some metrics), then policy and enforcement
    - Hybrid Option to default "guide" except for "high risk" organizations where policy and enforcement would be applied
- Monitoring component included or existing audit augmentation or any audit function?
- Central services vs. distributed services vs. hybrid approach (e.g. centralize costly "commodity based" services (e.g. Secure Operations Center), but leave unique (e.g. application) security to owning organization
- Critical infrastructure definition and support
- Privacy component(s)
- Business continuity (including "ruggedness"/resiliency)
- Leverage proven and "non-technical" best practice model for organizational measurement and roadmap to organizational security

The Subcommittee on State Structure and Best Practices Structure include the following members:

- Barbara Gonzalez, Subcommittee Co-Chair, Manager, Special Projects, NERC, Pepco Holdings, Inc.
- Joe Jarzombek, Subcommittee Co-Chair, Director, Software & Supply Chain Assurance, U.S. Department of Homeland Security Office of Cybersecurity and Communications
- Russell Butler, Executive Director/Attorney, Maryland Crime Victims' Resource Center, Inc.
- Fred Ferrer, Chief, Critical Infrastructure/Key Resources Branch, Anti-Terrorism Division, Maryland Coordination and Analysis Center
- Elizabeth Hight, Former Vice President, Cybersecurity Practice Hewlett Packard
- Robert Rosenbaum, Executive Director, Maryland Technology Development Corporation

The findings and recommendations of the Subcommittee on State Structure and Best Practices s are included in Appendix.

Subcommittee on Marketing and Partnerships

The Subcommittee on Marketing and Partnerships reviewed the state's role in promoting cyber innovation to develop recommendations for economic development, attracting private sector investment and job creation in cybersecurity. Based on the review conducted, the Subcommittee decided to focus on the following four areas:

- Define State's role in promoting cyber innovation
- Formulate recommendations for growth and economic development

- Articulate methods the State can use to promote coordination and collaboration to develop and grow the workforce needed in the science, technology, engineering, and mathematics (STEM) and cybersecurity.

The members of Subcommittee on Marketing and Partnerships are:

- Larry Letow, Subcommittee Co-Chair, TCM Chairman and President and COO & former Chair of the Maryland Tech Council
- Bel Leong-Hong, Subcommittee Co-Chair, Founder, President & CEO Knowledge Advantage Inc.
- Rick Geritz, CyberHive LLC
- Fred Ferrer, Chief, Critical Infrastructure/Key Resources Branch, Anti-Terrorism Division, Maryland Coordination and Analysis Center

Subcommittee on Education and Training

The Subcommittee on Education and Training reviewed the gaps and developed recommendations that the state may adopt to increase cyber innovation by enhancing and promoting cyber workforce training and education in Maryland.

The members of Subcommittee on the Education and Training Subcommittee include:

- Kathy Michaelian, Subcommittee Chair, Instructional Dean, Montgomery College
- Christian Anthony, The Johns Hopkins University Applied Physics Laboratory
- Rosemary Budd, Former President, Fort Mead Alliance
- Chieh-San Cheng, President and CEO, Global Science & Technology, Inc.
- Darrell Durst, Vice President, Lockheed Martin
- Sean Fahey, Research and Development Program Manager, John Hopkins University Applied Physics Laboratory
- Megan Ferguson, Knowledge Advantage Inc.
- Frederick Ferrer, Chief, Critical Infrastructure/Key Resources Branch, Anti-Terrorism Division, Maryland Coordination and Analysis Center
- Barbara Gonzalez, Manager - Special Projects, NERC, Pepco Holdings, Inc.
- Rear Admiral Elizabeth (Betsy) A. Hight (USN, Ret.), Former Vice President, U.S. Public Sector Cybersecurity Practice, HP Enterprise Services
- Joe Jarzombeck, Department of Homeland Security
- Kelly Koermer, Anne Arundel Community College
- Kent Malwitz, President, Chief Learning Officer at UMBC Training Centers
- Pat Mikos, Program Manager at Maryland State Department of Education

- Casey O’Brien, Executive Director, National CyberWatch Center
- Joseph Whittaker, Dean, School of Computer, Mathematical and Natural Sciences, Morgan State University

The findings and recommendations of the Subcommittee on Education and Training are included in Appendix.

V. Commission Activities

Process of Discovery

The Commission has been meeting regularly since November 22, 2011. The summaries, agendas, and presentations of all Commission meetings are available on the Commission’s website at http://www.umuc.edu/legal/cyber/. Following are the highlights of all Commission meetings:

June 26, 2014

Delegate Susan C. Lee reported on the 2014 General Assembly session, which she called a difficult session compared to what had been accomplished in 2013 on cybersecurity. However, she indicated that during the 2014 session, HB 806 which she introduced and was recommended by the Commission’s Legal Strategy Subcommittee, passed the Maryland General Assembly.

HB 806- Health Information Exchanges- Protected Information- Regulations: Recommended by the Commission's Legal Strategy Subcommittee, this legislation seeks to protect the privacy and security of health care information obtained or released through a health information exchange by requiring the Maryland Health Care Commission to adopt regulations that govern the access, use, maintenance, disclosure, and re-disclosure of protected health information as required by state or federal law, including the Federal Health Insurance Portability and Accountability Act (HIPAA) and the Federal Health Information Technology for Economic and Clinical Health Act (HITECH). The recent HIPAA Omnibus Rule added the term “maintain” to the scope of responsibilities of covered entities and business associates. The law would make the regulations consistent with HIPAA and HITECH and bring information held by cloud entities into the scope of those regulations. HB 806 was passed by the Maryland General Assembly and signed by Governor Martin O’Malley on May 15, 2014.

Delegate Lee indicated that the commission will be working on more proposed bills for the 2015 legislative session and asked members to provide recommendations to the Legal Strategy Subcommittee.

Elliot Schlanger, Director of Security and Chief Information Security Officer, Department of Information Technology, State of Maryland, reported that during 2014 the Maryland Department of Information Technology (DoIT) issued an annex to its master plan that deals with cybersecurity. The annex develops a baseline strategy that covers governance, the need for continuous assessment, and sets up a comprehensive training awareness program that helps build a culture of cybersecurity awareness throughout the state.

January 21, 2014

The following proposed bills were recommended and endorsed by the Commission to be introduced in the 2014 General Assembly session:

- SB 197/HB 804: Statewide Information Technology Master Plan Inclusion of Cybersecurity Framework –Requirement. This bill requires the statewide information technology master plan developed by the Secretary of Information Technology (IT) include a cybersecurity framework. The Secretary of IT must consider guidelines developed by the National Institute of Standards and Technology (NIST) in developing or modifying the Cybersecurity Framework and relating to the inclusion of a Cybersecurity Framework in the statewide information technology master plan.

- SB 386/HB 801: Commission on Maryland Cybersecurity Innovation and Excellence – Membership, Duties and Termination Date. The purpose of this proposed bill is to expand and further diversify membership of the Commission on Maryland on Maryland Cybersecurity Innovation and Excellence and extend its term beyond 2014.

- SB 249/HB 808: Commission on Maryland Cybersecurity Innovation and Excellence Duties. This proposed bill requires the Maryland Commission on Cyber Security Innovation and Excellence to study and develop strategies and recommendations for advancing telemedicine technologies and use; and generally relating to the duties of the Commission.

November 6, 2013

Delegate Lee briefed the Commission members on the cybersecurity-related bills introduced during the 2013 General Assembly session. Delegate Lee noted that it was a very good session in terms of passing two major pieces of legislation dealing with cybersecurity. The first bill deals with protecting our state databases against cyber attacks and notifying our citizens when there is a breach of our personal information held by state agencies. The second bill deals with protecting our healthcare and health records from identity theft. This was a timely bill not only because it took effect on October 1, 2013 when the new health benefit exchange was launched, but also because of the myriad of identity theft crimes that could be committed as Maryland and the country rapidly move toward electronic health and health care records. As it may now be easier to steal or alter those records on a large scale, thereby exposing patients to being billed for medical services they did not receive; death or injury caused by altered information; the denial or limiting of benefits by providers or insurers; drugs being incorrectly prescribed or purchased in their name; and debts appearing on their credit reports they did not incur, the new legislation allows for the effective deterrence and prosecution of those crimes.

While there is still a need for improvement, this legislation is a great step forward in protecting our citizens' sensitive data.

Lynn Garland, an online voting system expert, briefed the Commission on the topic of securing ballots requested via online. She indicated that elections are targets of fraud and Maryland's planned online absentee voting system may be vulnerable. She recommended that we should continue to strive to improve voter access through technology. However, we should not implement systems until the issues of authentication, privacy and security are addressed.

Karen Morgan, Principal Analyst and Sally Guy, Policy Analyst, Department of Legislative Services presented findings from a report on the state of identity theft in Maryland including the laws that have been passed and some of the challenges that are faced by law enforcement in investigating and fighting identity theft. According to the report, the State and federal law enforcement are not able to respond in a timely manner. The report indicates that coordination between federal and state law enforcement has been a significant help in dealing with identity theft.

Corporal Jeffrey Shackelford from the Maryland Coordination and Analysis Center, Anti-Terrorism Advisory Council of Maryland briefed the Commission on the Sovereign Citizen Movement and its threat.

June 11, 2013

Delegate Susan Lee and Senator Catherine Pugh briefed the Commission and noted that important legislation proposed by the Commission and its Legal Strategy Subcommittee passed the Maryland General Assembly, namely SB 676/ which was crossed filed with HB959, SB 624 / HB 942, and SB 776/ HB 934. Respectfully, these first ever Maryland laws set forth provisions for protecting citizens against the theft or misuse of their sensitive personal information held by state government agencies and provide requirements for agencies for notifying them when there is a breach; a law to protect against patients and heath care professionals from a myriad of identity theft crimes that may occur from the theft or misuse of health and health care information by allowing for the prosecution of those crimes; and a law to move forward the Telemedicine Task Force that has been instrumental in moving to the forefront strategies and recommendations for advancing and yielding the full benefits of cutting edge telemedicine and telehealth which have track records of saving lives, improving outcomes, reducing health care disparities and costs.

Scott Jenson, Deputy Secretary, Department of Labor, Licensing and Regulation (DLLR) briefed the Commission on the new bill called the Employment Advancement Right Now (EARN). The EARN is a $4.5 million workforce development grant program. He indicated that it is a competitive grant and DLLR is in the process of seeking applications and setting up apparatus necessary for implementing and managing the grant.

The Director of the Healthcare Information Exchange Regulations, Department of Health and Mental Hygiene, Dr. David Sharp briefed the Commission and noted that they have made significant progress in the state of Maryland in terms of infrastructure to advance healthcare related information technology. However, there are some challenges in protecting sensitive information of consumers. Presently, there is a lack of granularity controls that allow the consumers to fully protect their information. Delegate Susan Lee proposed a motion to send a letter to Dr. Sharp about including language regarding maintained data. The Commission passed the motion and a letter was sent to Dr. Sharp.

January 29, 2013

The Commission members, Dr. Greenberger and Karen Morgan, discussed the memorandum of Subcommittee on Legal Strategy to strengthen the provisions of the Maryland Personal Information Protection Act (MPIPA). Ms. Morgan stated that the Commission had proposed two modifications to strengthen the provisions of MPIPA: 1) changing the definition of encryption to make it stronger and 2) adding a component called private information which captures detailed information such as social security number, driver’s license and state issued identity cards.

The Commission by unanimous vote of all members present approved a motion to adopt concepts and recommendations provided in the memorandum of Subcommittee on Legal Strategy aimed at strengthening the provisions of MPIPA against identity theft and to providing prompt notice when violations occur.

Edward Shulder, Manager of Legislative Audit, Department of Information Technology (DoIT) commended the Commission’s effort to change the law to include government agencies along with businesses. He indicated that DoIT would work with state agencies to ensure they comply with requirements of information security.

Dr. David Sharpe, Director of the Maryland Healthcare Commission Center for Health Information Technology briefed the Commission on the importance of Health Information Technology (HIT) in terms of patient care and efficiencies in healthcare. He informed the commission that the Maryland Chesapeake Regional Information System was designated as the statewide HIT in 2009. There are relatively complicated algorithms that are utilized such that specific patients can be recognized and identified and the data is encrypted. He indicated that the technology is being embraced by the hospitals and physicians.

December 6, 2012

William Van Horne, who is Chief Counsel of the United States Senator Benjamin Cardin, addressed the Commission about the field hearings in Laurel, MD led by Senator Cardin. He indicated that the hearings focused on how businesses, incubators such as the Chesapeake Innovation Center and Maryland universities in partnership with the US Cyber Command, National Security Agency (NSA), National Institute of Standards and

Technology (NIST) and other federal agencies can engender a strong cybersecurity industry in Maryland to the overall benefit of the nation.

June 8, 2012

Bridgette Smith, who is a legislative aide to Congressman John Sarbanes, addressed the Commission and noted that the Congressman Sarbanes appreciates that the internet has become critical to innovation and economic growth for communities and individuals and he believes that cyberspace can be protected without compromising its usefulness. Congressman Sarbanes has been active on a wide spectrum of projects related to cybersecurity. These include securing a) $6 million in funds for physical infrastructure improvements to support the larger workforce at Fort Meade, b) $2.3 million for upgrades on Ft. Meade itself, c) a $4.9 million U.S. Department of Labor grant to the Anne Arundel Economic Development Corporation and Ann Arundel Community College for training an estimated 1,000 people over a three-year period in cybersecurity, and d) the Office of Economic Adjustment funding for the Ft. Meade Regional Growth Committee.

Ms. Smith briefed the Commission on a number of bills that the US House of representatives had sent to the US Senate concerning cybersecurity, including Federal Information Security Amendments Act (HR 4257), Cyber Security Enhancement Act (HR 2096) and Advancing America's Networking and Information Technology Research and Development Act (HR 3834).

Pam Walker, Director of Government Affairs, National Association of State Chief Information Officers, presented key findings of the Deloitte – NASCIO survey of state Chief Information Officers (CIOs) in 2012. This survey covered a number of key areas such as information security, governance, role and structure of the Chief Information Security Officer (CISO), identity and access management.

March 13, 2012

The Commission Co-Chair, Delegate Susan Lee framed the importance of the Commission and its efforts. She praised the leadership of the Governor and noted that the State has taken steps forward on the issue of cybersecurity. The purpose of the Commission is to support this effort by developing a roadmap that has at least two components. The first is to provide comprehensive legislative and policy recommendation for protecting the operations of the state, commercial institutions, economy, and infrastructures against cyber attacks. The second is to provide recommendations and strategies for advance cyber innovation and jobs, help education institutions at all levels create a pipeline for cyber jobs, and make Maryland the epicenter of cyber security.

The Commission members discussed the legislative mission of the Commission and outlined its structure organized around the four main themes: legal strategy, state structure and practice, marketing and partnerships, and education and training.

The Assistant Secretary of Marketing and Communication, Andrea Vernot, briefed the Commission on the state's efforts in attracting cybesecurity companies to Maryland. She noted the aggressive and wide-ranging nature of this activity, including a state presence at large trade shows and expos such as RSA conferences and online marketing. In the past two years 50 new firms had been attracted to Maryland, generating jobs and well over $100 million in investments.

The Maryland House Speaker, Michael Busch, addressed the Commission. He commended the strong leadership at the state level and within Maryland's US Senate and House of Delegates on cybersecurity issues. He emphasized the urgency around cybersecurity both for the state and the nation and the need to recruit the best and the brightest cyber talent for work in this region.

November 22, 2011

Senator James E. DeGrange and Delegate Susan Lee welcomed the Commission members and thanked them for their service. Delegate Lee provided information regarding HB 665 which authorized the Commission, as well as her earlier passed 2010 legislation, HB 778, which amended § 7-302 of the Criminal Law article and provided for greater penalties to individuals who are guilty of unauthorized access to computers and related materials which interrupt or impair the state government or public utilities.

The meeting was dedicated to an open discussion on the goals of the Commission. The following three main goals were highlighted:

- Although the Commission should not recreate what is already available, it is important to collect information on the various cybersecurity initiatives currently occurring in Maryland so they can be catalogued.
- In terms of future planning for cybersecurity initiatives, the Commission members recognize the strengths that Maryland already has in this area and will work to identify the gaps. By looking at these gaps, the Commission will study and propose how the gaps can be addressed.
- The educational element of cybersecurity issues and how important it is for the general population to understand what cybersecurity is and how individuals should protect themselves from potential threats.

Awareness Raising & Outreach

For the last three years, the Commission has hosted the following open receptions for legislators in the beginning of the General Assembly sessions at the House Office Building in Annapolis, Maryland. The reception agendas and details are available on the Commission's website at: http://www.umuc.edu/legal/cyber/.

2014 Annual Reception

The Commission hosted its third annual reception on January 21, 2014. The reception was led and moderated by Delegate Susan Lee and Senator Catherine Pugh, Co-Chairs of the Commission on Maryland Cybersecurity Innovation and Excellence. Congressman John Delaney, Congresswoman Donna Edwards, and Maryland Attorney Douglas F. Gansler addressed participants of the reception about the role and importance of cybersecurity in the state of Maryland. In addition to Commission members, the following legislators attended the reception:

- Senator Brian Frosh
- Delegate Ana Sol Gutierrez
- Delegate Tawanna Gaines
- Delegate Glenn Glass
- Delegate Kumar Barve
- Delegate Barbara Robinson
- Delegate Doyle Niemann
- Delegate Melony Griffith
- Delegate Jolene Ivey
- Delegate Bonnie Cullison
- Delegate Dan Morhaim
- Delegate Geraldine Valentino-Smith
- Delegate Veronica Turner
- Delegate John Bohanan
- Delegate J. Wood
- Delegate Talmadge Branch
- Delegate Cheryl Glenn
- Delegate David Fraser-Hidalgo
- Delegate Keiffer Mitchell
- Delegate Shawn Tarrant
- Delegate Susan Krebs
- Delegate Addie Eckardt

2013 Annual Reception

The Commission hosted its second annual reception on January 29, 2013. Maryland Attorney General Doug F. Gansler addressed the participants of the reception about cybersecurity as a national issue and as an opportunity for Maryland to grow economically through innovation in this sector. This was an open reception joined by Commission members, general public and many members of the Maryland state Senate and the House of Delegates.

2012 Annual Reception

The Commission hosted its first reception on March 13, 2012. Senator Catherine Pugh welcomed members of the General Assembly, the Governor’s Office, the

Commission and the general public to the Commission’s Open House. She commented on the importance of cybersecurity as an issue and commended Delegate Susan Lee on her leadership and efforts to establish the Commission.

Senator Catherine Pugh introduced the Commission’s special guest, US Congressman Dutch Ruppersberger, Maryland’s 2nd District. Congressman Ruppersberger spoke at length about the nature of the cyber threat to the nation, the legislative activity in Congress, the importance of the partnerships between industry, the universities and government agencies in creating the tools to enhance cyber security and the critical need for science, technology, engineering, and mathematics (STEM) education. He pointed to the major role that US Senator Barbara Mikulski has played nationally on cybersecurity issues and underscored the important opportunities that cyber offers Maryland and the contributions that the state is making and will continue to make in supporting the nation’s cybersecurity efforts.

This was an open reception attended by general public, Commission members and many members of the Senate and the House of Delegates.

Briefing the German Federal Republic Delegation

Delegate Susan Lee briefed a delegation from the German Federal Republic (BDR) about the Commission and its efforts in assisting the state of Maryland to become the epicenter of cybersecurity. The delegation was invited to the United States under the auspices of the Department of State's International Visitor Leadership Program. The meeting was held on June 13, 2013 at the University of Maryland University College (UMUC). The meeting was arranged in conjunction with the World Trade Center Institute and UMUC. The German Delegation included the following:

- Christian Heinz, Spokesman, Data Protection, Christian Democratic Union Caucus, Hesse State Parliament
- Sebastian Michael Meissener, Senior Legal Advisor and Deputy Head of the European Privacy Seal Department, Office of the Data Protection Commissioner, Independent State Center for Data Protection, State of Schleswig-Holstein.

The details and presentation of the briefing are available on the Commission’s website at: http://www.umuc.edu/legal/cyber/.

CyberMaryland Luncheon: A Cybersecurity Awareness Event

The Commission on Maryland Cybersecurity Innovation and Excellence and the Cybersecurity Advisory Board of the Maryland Department of Business and Economic Development (DBED) held a joint luncheon. This luncheon was held during the Cybersecuyrity Awareness Month on October 16, 2012 at the CyberMaryland Conference in Baltimore Convention Center. The event was instrumental in enhancing the Cybersecuyrity Awareness among the leadership of public and private sector organizations in Maryland.

The CyberMaryland Luncheon featured the following speakers:

- Barbara Mikulski, United States Senator
- Lt. General Harry Raduege, United States Air Force (Ret.), Chairman of the Deloitte Center for Cyber Innovation

The event provided an excellent opportunity for networking and exploring collaborations among leaders of public and private organizations in the area of cybersecurity. UMUC supported the CyberMaryland Luncheon as part of its cybersecurity initiative.

VI. Commission Legislative Accomplishments

The Commission on Maryland Cybersecurity Innovation and Excellence has been instrumental in proposing and passing the following cybersecurity-related legislation. The Commission commends the state legislature for passing bills during its tenure that will better enable state agencies and industry to secure their domains of cyberspace.

- **SB 676/cross filed with HB 959- Governmental Procedures-Security and Protection of Information.** This bill was passed by the General Assembly, signed into law Governor Martin O'Malley on May 2, 2013, and went into effect on July 1, 2014. The law sets forth provisions for protecting citizens' personal information held by state government agencies (including local government units) and notification requirements when there is a breach. The judicial and legislative branches which were deleted from the bill out of concerns expressed by those branches that the judiciary and legislative branches have unique issues and challenges in protecting their data, including the costs involved. There was discussion about future legislation more tailored to each governmental branch.

- **SB 624/HB 942: Identity Fraud – Health Information and Health Care Records.** This bill was passed by the General Assembly, signed into law by Governor Martin O'Malley on May 2, 2013, and went into effect on October 1, 2013. SB 624/ HB 942 expands the identity fraud statute to include "health information" and "health care." The protected health information (PHI) has become valuable information for those wanting to commit criminal acts. Criminalizing this conduct now allows prosecutors to prosecute these offenses of fraudulent use or possession of PHI, as well as to allow victims of this conduct to seek restitution. Under the law, a person may not:
    - Knowingly, willfully, and with fraudulent intent possess, obtain, or help another person to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to access health information or health care in the name of the individual;
    - Knowingly and willfully assume the identity of another person, including a fictitious person, with fraudulent intent to access health information or health care; and

- Knowingly, willfully, and with fraudulent intent use a re-encoder or a skimming device to engage in specified activities in order to access health information or health

- **HB 806: Health Information Exchanges - Protected Health Information Regulations.** Recommended by the Commission's Legal Strategy Subcommittee, this legislation seeks to protect the privacy and security of health care information obtained or released through a health information exchange by requiring the Maryland Health Care Commission to adopt regulations that govern the access, use, maintenance, disclosure, and re-disclosure of protected health information as required by state or federal law, including the Federal Health Insurance Portability and Accountability Act (HIPAA) and the Federal Health Information Technology for Economic and Clinical Health Act (HITECH). The recent HIPAA Omnibus Rule added the term “maintain” to the scope of responsibilities of covered entities and business associates. The law would make the regulations consistent with HIPAA and HITECH and bring information held by cloud entities into the scope of these regulations. HB 806 was passed by the Maryland General Assembly and signed by Governor O’Malley on May 15, 2014

VII. Other Commission Proposed Legislation

The Commission proposed the following bills, which did not move forward during the General Assembly sessions of 2013 and 2014.

2014 Proposed Legislation

- **SB197 / HB 804 Statewide Information Technology Master Plan Inclusion of Cybersecurity Framework –Requirement:** The bill required the statewide information technology master plan developed by the Secretary of Information Technology (IT) to include a cybersecurity framework. The Secretary of IT must consider materials developed by the National Institute of Standards and Technology (NIST) in developing or modifying the cybersecurity framework; and relating to the inclusion of a cybersecurity framework in the statewide information technology master plan.

- **SB 368 / HB 801 Commission on Maryland Cybersecurity Innovation and Excellence – Membership, Duties and Termination Date**. The bill required the expansion and further diversification of membership of Commission on Maryland Cybersecurity Innovation and Excellence and proposed the extension of its term beyond 2014.

- **SB 249 / HB 808 Commission on Maryland Cybersecurity Innovation and Excellence Duties:** The bill required the Commission on Maryland Cybersecurity Innovation and Excellence to study and develop strategies and recommendations for advancing telemedicine technologies and use; and generally relating to the duties of the Commission on Maryland Cybersecurity Innovation and Excellence.

2013 Proposed Legislation

- **SB 859/HB 960 Maryland Personal Information Protection Act- Revisions:** SB 859/HB 960, which applied to businesses, received an unfavorable report by the Economic Matters Committee and, thus, did not move forward. Some businesses opposed the bill because of concerns it may heighten existing standards regarding the protection of personal information. Businesses were concerned, for example, that the definition of "personal information" was too broad and that the legislation would create an additional financial burden. Thus, the standards of the existing breach notification law remain the same.

- **SB 494/HB 937 Commission on Maryland Cybersecurity Innovation and Excellence – Duties:** SB 494/HB937 required the Commission to study and develop specified strategies and recommendations for advancing telemedicine technologies and use, including (1) methods of supporting innovation, development, and investment in the emerging technology; (2) the role of telemedicine in reducing health care disparities and addressing primary care and specialty care provider shortages across the continuum of care; (3) the protection of databases in the use of telemedicine; and (4) any other issue related to advancing and supporting telemedicine technologies and use.

VIII. Findings & Recommendations

The two main components of the Commission's charge include: (1) to conduct an overview of current state, federal, and international laws in order to provide recommendations for laws and/or policies; and (2) to provide a strategic roadmap for making Maryland the leader in cybersecurity innovation and job creation. To address these two main components, the Commission is organized around four main themes: legal strategy, state structure and practice, marketing and partnerships, and education and training. Therefore, the Commission's findings and recommendations are organized accordingly as follows:

Legal strategy

A comprehensive review of current state, federal, and international laws was conducted to identify statutory gaps that may be addressed by State legislation. The Commission's key findings and recommendations in this regard are as follows:

Findings

- The Commission has been instrumental in passing major pieces of first ever legislation in the state to protect sensitive data held by state agencies against cyber attacks; to protect health and health care records from identity theft; and to protect the privacy and security of protected health information. However, there is a need for more comprehensive cybersecurity legislation to improve cybersecurity protections in Maryland and to become the epicenter of cyber innovation and job creation.

- President Obama issued Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” on February 12, 2013. The aim of Executive Order is to strengthen the resilience of critical cybersecurity infrastructure. However, federal executive orders often cannot achieve, due to legal limitations, everything a passed piece of legislation can. Through an executive order, the Obama administration can only use existing law to engage the nation’s critical infrastructure entities to promote new and voluntary security enhancements. To strengthen the state’s cybersecurity infrastructure and protect the information of citizens and businesses within its borders, there is a need for passing state legislation in Maryland to support and further reinforce the Executive Order.

- The Maryland Personal Information Protection Act (MPIPA) was enacted to help ensure that Maryland consumers’ personal identifying information is reasonably protected, and in the case of a breach, the consumer is notified so that they can take measures to protect themselves. While it has provided many essential safeguards, Maryland can take a step towards more robustly protecting itself and its citizens by amending certain provisions of the MPIPA.

Recommendations

- The State of Maryland should consider passing state legislation to support the Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity,” issued by President Obama on February 12, 2013. The Commission provides the following specific recommendations for Maryland to support and further reinforce the executive order:

- A Maryland Cybersecurity Council should be established with members from various state agencies such as the Governor’s Office of Homeland Security (GOHS), the Department of Information Technology (DoIT), the Maryland Coordination and Analysis Center (MCAC), the Maryland Department of State Police (MDSP), the Maryland National Guard (MNG), the Maryland Defense Force, the Maryland Emergency Management Agency (MEMA), and the Maryland Department of Transportation (MDOT). These State agencies would work with National Institute of Standards and Technology (NIST), other Federal partners, private sector owners and operators and other private cybersecurity experts as follows:
    - For all critical infrastructure not covered by Federal law or executive order, the proposed Maryland Council would conduct risk assessments to determine which infrastructure sectors are at the greatest cyber risk and need the most urgent enhanced cybersecurity measures.
    - The proposed Maryland Council would use Federal guidance from NIST to identify categories of critical infrastructure as critical cyber infrastructure if cyber damage or unauthorized cyber access to that infrastructure could reasonably result in catastrophic consequences such as interruption of life-sustaining services including energy, water, transportation, emergency services, or food, sufficient to cause a mass

    casualty event or mass evacuations, catastrophic economic damage, or severe degradation of state or national security.
  - The proposed Maryland Council should work with the critical infrastructure entities not covered by the cybersecurity executive order to strengthen its cybersecurity by assisting these entities in complying with federal cybersecurity guidance.
  - The proposed Maryland Council should work with private sector cyber security industry members and other experts to adopt, adapt, and implement the federal NIST cybersecurity framework of standards and practices.

- The state should develop legislative incentives for businesses to successfully participate in the NIST Cybersecurity Framework and receive certification by the Federal government as follows:
  - State liability protection should be given from any punitive damages directly arising from an incident related to a cyber risk if in full compliance of adopted cybersecurity practices.
  - Priority to technical assistance on cyber issues from the State
  - Receive real-time cyber threat information from the State.

- To improve information sharing, monitoring, and countermeasures, the Maryland state government should fully participate in the cyber information-sharing exchanges with the federal government and private companies

- The Cybersecurity legislative proposals have been scrutinized and often been found lacking in privacy and civil liberties protections by such organizations as the Constitution Project and the American Civil Liberties Union. The privacy and civil liberties should remain the vanguard for any future cybersecurity bills. The Maryland private critical infrastructure entities should adopt similar privacy protections as follows:
  - There should be a provision that information collected by Maryland may be used for only cybersecurity purposes, including prosecution of cybersecurity crimes, or to protect individuals from imminent threats of death or serious bodily harm and to protect children from sexual exploitation and serious threats to their physical safety. The information obtained may not be used for state security purposes or criminal prosecutions unrelated to cybersecurity.
  - The scope of information that may be shared with or by Maryland should be narrow and limited to that which is "reasonably necessary to describe" a cybersecurity threat indicator, so that companies cannot send massive quantities of private information unrelated to demonstrating a cyber threat. The bill should include a requirement that private companies make "reasonable efforts" to remove unrelated personal information that can identify a specific individual before sharing data with the government.

- All new guidelines and model practices set forth by NIST and the federal government should be evaluated, adapted, and adopted within a short reasonable amount of time by the proposed Maryland Cybersecurity Council.

- If possible, procurement and vendor preference should be afforded to companies that have been certified by the federal government as compliant with the highest cybersecurity standards.

- The cybersecurity education, recruitment and workforce development must be emphasized to comply with and complement the National Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology (NIST). It is critical that Maryland state and local governments adopt laws and policies that endorse and encourage cyber education in Maryland's high schools, colleges, and universities. In addition, it is critical to endorse and incentivize businesses and state and local government agencies to recruit, hire, and train people to excel in the cybersecurity field. The emphasis on cyber related education, recruitment, and workforce development will not only increase the cybersecurity of Maryland, but it will allow Maryland the opportunity to be a leader in this emerging and vital field. The Commission's more specific recommendations in this regard are as follows:
    - A study should be conducted on the state of cybersecurity education in institutions of higher learning in Maryland including such items as:
        - the extent of professional development opportunities for faculty in cybersecurity principles and practices;
        - descriptions of the content of cybersecurity courses in undergraduate computer science curriculum;
        - the extent of the partnerships and collaborative cybersecurity curriculum development activities that leverage industry and government needs, resources, and tools; and
        - proposed metrics to assess progress toward improving cybersecurity education.
    - Implement outreach and awareness programs on cybersecurity to develop and recruit talent.
    - Establish a program to conduct competitions and challenges of high school students, college students, graduate students, veterans, and others, that seek to identify, develop, and recruit talented individuals to work in State and local government agencies, and the private sector to perform duties relating to the security of the state information infrastructure
    - Create a Maryland cyber scholarship-for-service program.
    - Assess the readiness and capacity of State and local workforce to meet the cybersecurity mission of the Federal and Maryland Government. Develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of cybersecurity personnel of the State Government.

- Maryland should increase the effectiveness of the Maryland Personal Information Protection Act (MPIPA) by (1) closing loopholes to increase the legislation's applicability; (2) addressing ambiguous provisions in the notification process; (3) eliminating the encryption exemption; and (4) clarifying the term "reasonable security procedures and practices." More specific recommendations, with specific reference to the MPIPA language that needs to be amended to increase the effectiveness MPIPA, are provided on the Commission's website at: http://www.umuc.edu/legal/cyber/. The Commission proposed and introduced a bill (HB 960/SB 859, Maryland Personal Information Protection Act – Revisions) in this regard in the 2014 Session of the Maryland General Assembly. However, it did not move forward in the House and Senate. The commission recommends introducing this bill with further refinement in the 2015 Session of the Maryland General Assembly.

- Maryland should reinforce and support the inclusion of NIST Cybersecurity Framework in Statewide Information Technology Master Plan. The legislation should require state to include a cybersecurity framework in the statewide information technology master plan developed by the Secretary of Information Technology (IT). The Secretary of IT must consider guidelines developed by the National Institute of Standards and Technology (NIST) in developing or modifying the cybersecurity framework; and relating to the inclusion of a cybersecurity framework in the statewide information technology master plan. The Commission introduced a bill (SB 197/HB 804: Statewide Information Technology Master Plan Inclusion of Cybersecurity Framework –Requirement) in this regard in the 2014 Session of the Maryland General Assembly. However, it did not pass the House. The commission recommends introducing this bill with further refinement in the 2015 Session of the Maryland General Assembly.

- There is a critical need to study and develop strategies and recommendations for advancing telemedicine technologies and use in the State of Maryland. The commission recommends a bill that will require the Commission to study and develop strategies and recommendations for advancing telemedicine technologies and use; and generally relating to the duties of the Commission. The Commission drafted and introduced a bill (SB 249/HB 808: Commission on Maryland Cybersecurity Innovation and Excellence-Duties and Memberships) in this regard in the 2014 Session of the Maryland General Assembly. However, it did not pass the House Economic Matters Committee. The Commission recommends introducing this bill with further refinement in the 2015 Session of the Maryland General Assembly.

- The Commission on Maryland Cybersecurity Innovation and Excellence has been instrumental in passing legislation aimed at protecting the information infrastructure; enhancing cybersecurity awareness among the legislatures and general public; and formulating strategic recommendations for making

Maryland the leader in cybersecurity innovation and job creation. The Commission is committed to making further progress and continue to assist the State in protecting our government, economy, and infrastructures from cyber attacks and developing strategies for promoting innovation, technology transfer, and pipelines for cyber jobs at all levels. To continue its critical work, the Commission recommends the extension of its term beyond 2014.

State Structure and Best Practices

The Commission reviewed the many resources, programs, best practices, and opportunities that already exist in Maryland and the US Federal Government that might be leveraged by State agencies. To formulate findings and recommendations, the Commission aligned State priorities with national priorities for critical infrastructure security and resilience; reviewed means for leveraging relevant national programs, initiatives, and standards; and reviewed applicable performance audit reports of the Department of Information Technology (DoIT) and selected State agencies. The key findings and recommendations in this area are as follows:

Findings

- The State needs to focus more on implementing the existing cyber security practices and improving oversight in the State. One of the key concerns is about the apparent lack of progress made by DoIT and State agencies in response to the performance audit findings and recommendations included in the report by the Office of Legislative Audits, Department of Legislative Services, Maryland General Assembly. Focused on information system data security, the findings of the audit are as follows:
    - Current state law governing certain protections for personal identifiable information did not apply to state agencies.
    - DoIT did not have a formal process in place to enforce the provisions of its information security policy.
    - DoIT could improve guidance to help agencies address certain security issues.
    - DoIT needs to develop a more responsive process to address emerging technologies and a policy regarding mobile devices.
    - DoIT had not developed recommended practices for implementing data loss prevention solutions.
    - State agencies often did not document the security categorization of information systems.
    - Certain agencies' information security policies were not agency specific or did not include all required components.
    - Risk management processes were not fully implemented.
    - Security awareness training was not always provided to employees or tracked.
    - Data contained on portable devices was not always properly protected use of certain information security best practices.

    - State agencies were in various stages of implementing data loss prevention tools and techniques.
    - State agencies had varied practices in implementing vulnerability scanning and penetration testing.

    - With the exception of security awareness training being provided to all employees and being tracked, it is not readily apparent to what extent DoIT and State agencies are following-up in response to the performance audit recommendations.

- The Commission realized that many models, frameworks and standards are available to guide process improvement and assess cyber security capabilities. However, each sector and agency has a different set of mission and business priorities.

Recommendations

- DoIT and State agencies should provide an update progress report in response to the findings and recommendations of the September 2012 Performance Audit. The Commission offers the following specific recommendations in this regard:
    - As a minimum, for each of the audit findings, DoIT and/or the respective State agencies should provide an update on implementation status with respective timelines for the associated remedies, or justifications as to why full implementation has yet to be realized.
    - The update progress report should include details about how DoIT and State agencies are monitoring and tracking performance relative to the NIST Cybersecurity Framework and the Critical Infrastructure Cyber Community (C3) Voluntary Program.
    - As part of that update, DoIT and each State Agency should specify which NIST 800-53 rev4 security controls are used; indicating how selected controls address priorities aligned with citizen protection, privacy, operational support (and mission continuity), and, as applicable, law enforcement.

- The Chief Information Security Officer (CISO) should have an independent reporting path to top State leadership, independent of the Chief Information Officer (CIO), to provide status updates and advise on the cyber resilience of Maryland’s IT infrastructure.

- DoIT should establish a comprehensive State-wide Incident Response Process and Capability, initially under the CISO for the State. While DoIT and each State agency will have incident response capabilities, it is important to understand that no single organizational entity would have the capability to adequately address the growing threat associated with cyber attacks. Information sharing for threat analysis and incident management is needed among State organizations, in coordination with industry and US Government departments and agencies.

- DoIT, in coordination with industry, should establish a program for developing the capability to track and report on the cyber resilience of Maryland's critical infrastructure, including all State agencies. This should be done consistent with the Critical Infrastructure Cyber Community (C3) Voluntary Program that uses a unified approach to cyber risk management for critical infrastructure sectors, and this includes State agencies and industry that operates infrastructure upon which citizens rely for critical services. The approach organizes Cybersecurity Framework-related awareness and engagement based on the priority risks to each sector.

Marketing and Partnerships

The Commission reviewed the State's role and efforts in promoting cyber innovation, economic development, private sector investment and job creation in cybersecurity. The Commission's key findings and recommendations in this regard are as follows:

Findings

- The Commission recognizes the strengths that Maryland already has in the area of cybersecurity. It is important to collect information on the various cybersecurity initiatives currently occurring in Maryland so they can be catalogued and promoted.

- The State can play more significant role in supporting and promoting cyber innovation to enhance the creation of more jobs in Maryland.

- There is a need for better coordination and utilization of state and federal resources to attract private sector investment and job creation in cybersecurity.

- There are sixteen higher education institutions and eight 2-Year academic institutions recognized by the National Security Agency and the Department of Homeland Security as National Centers of Academic Excellence in Information Assurance Education (CAE/IA). This makes Maryland the leading State with one of the largest concentration of academic institutions with the designation of CAE/IA. There is a lack of State-level marketing and positioning of state educational institutions as the nation's leaders in premier cyber education, innovation and technology.

- The State needs to support and adopt more effective ways to promote collaboration and coordination among cybersecurity industry and higher education institution in Maryland.

Recommendations

- The State should play a leading role in promoting cyber innovation and job creation that is based on the work of the Department of Business and Economic Development (DBED) released in the form of a report titled CyberMaryland. The report can be access at: http://issuu.com/cybermaryland/docs/cyberreport?e=1502745/2646192.

- The State should encourage and support public-private partnerships, help companies to leveraging federal funds for research development to producing and commercializing innovative cyber technologies.

- There should be centralized approach to gathering, disseminating and promoting information on the various cybersecurity initiatives and efforts occurring in Maryland. The Commission's website has been disseminating some information in this regard. However, more extensive effort is needed to develop a state portal hosting and promoting the various cybersecurity initiatives occurring in Maryland.

- The State may consider expanding existing resource centers similar to the CyberWatch Center Clearinghouse or CyberMaryland that includes regularly updated environmental and curricula scans.

- The State should develop a marketing plan highlighting the achievements of Maryland's educational institutions including the highest number of academic institutions recognized by the National Security Agency and the Department of Homeland Security (NSA/DHS) as National Centers of Academic Excellence in Information Assurance Education (CAE/IA). This would help in attracting cyber companies to Maryland, as they would be able to find high quality cyber talent developed in these premier Maryland's academic institutions that are recognized by NSA/DHS as CAE/IA.

Education and Training

The Commission reviewed resources, programs, best practices, challenges and opportunities of cybersecurity workforce training and education that already exist in Maryland and developed recommendations that will assist the State to increase cyber innovation by promoting workforce training, education, and development. The Commission's key findings and recommendations in this regard are as follows:

Findings

- The academic programs offered by State higher education institutions do not often complement, and sometimes compete with one another. Presently, the academic institutions face difficulties articulating computer science and cybersecurity programs between community colleges and 4-year academic institutions.

- There is a tremendous shortage of qualified teachers in areas of science, technology, engineering, and mathematics (STEM) and cybersecurity, particularly at high schools and community colleges.

- The high school curriculum does not offer the broadest exposure to computer science and cybersecurity. Only 61% of Maryland high schools offer computer science courses and less than half of all high schools offer more advanced computer science or programming courses.

- There is a lack of agility in the college and university computer science programs. The inclusion of software assurance and new programming languages in the curriculum is needed.

- There is a small pool of interested and prepared students at the beginning of the STEM and cybersecurity workforce pipeline. The existing pool of students in Maryland does not have the STEM and cybersecurity education and skills necessary to become part of the critical cyber workforce needed to protect the critical information infrastructure of the State.

Recommendations

- The most effective and sustainable solution to address the critical shortage of cybersecurity professionals is to expose and encourage as many kids at K-12 level to computer science (CS) education as early as possible. If there are large numbers of CS students flowing into the community colleges and 4-year institutions, a certain percentage of them will be attracted to the field of cybersecurity. The Commission recommends that the State should:
    - Provide funding to support the creation of Computer Science Certification programs in Maryland colleges and universities to facilitate the adequate preparation and credentialing of high school computer science teachers. Provide funding to support students interested in pursuing this program.
    - Incentivize the process to get more current teachers in Maryland's secondary schools certified in computer science and cybersecurity. Incentives could be financial or other such as sabbaticals, externships, use of community college classes to meet certification requirements, etc.
    - Include computer science and cybersecurity courses as options for students of the required Maryland State Department of Education Technology Education credit for high school graduation.
    - Expand ongoing cyber-awareness, including cyber ethics and cyber safety, activities and requirements in K-12.
    - Expand MD Virtual Online offerings. The offerings are currently limited to an applied computer science and an Oracle 3 database course. Additional computer science and cybersecurity courses are

under development and will be available starting in the 2014-2015 school year.
    - Expand co-curricular programs and transformative types of activities.
    - Develop online cyber education for Maryland K-12 students.
    - Leverage and support the National Science Foundation funded Computing Education for the 21st Century (CE21) program (http://ce21maryland.umbc.edu/).

- To enhance academic innovation and collaboration in Maryland, the State should provide encouragement, resources and institutional funding that will:
    - Lead to all of Maryland's educational institutions (K-16) with cybersecurity related programs mapping outcomes to common standards.
    - Lead to streamlined statewide articulations between high schools, community colleges, and four-year school programs (2+2+2).
    - Incentivize the creation of curriculum and expansion at selected University System of Maryland (USM) universities that articulates with the community college cybersecurity associate degree (AAS) curriculum to provide pathways to bachelor's degree for students. Some articulations in this regard already exist at the University of Maryland University College, Bowie State University, and Capitol College.
    - Assure that community colleges and universities incorporate software assurance concepts into their computer science curricula.
    - Develop academic pathways and bridge programs for students changing their educational focus.
    - Incorporate cyber related concepts across the curriculum (for example in business, psychology, and ethics).

- To create multiple pathways to cybersecurity employment in Maryland, the state should:
    - Create and support multiple pathways to job roles, not just necessarily the bachelor's degree.
    - Encourage portfolio review (military/work experience, industry certifications, etc.) as a substitute for degree attainment alone.

- The State should support and incentivize industry to partner with academic institutions for developing innovative ways to support student learning in the area of cybersecurity by:
    - Involving industry in teacher exchanges, externships, and mentorships for both students and teachers.
    - Expanding co-curricular programs and transformative type of activities involving industry. For example, afterschool programs, field trips, clubs, and competitions.
    - Incentivizing businesses to hire student interns in the area of cybersecurity.

- Using the existing Maryland Business Roundtable to create a sub-group focused on cybersecurity and computer science education and workforce development.

IX. Conclusion

Maryland having within its borders eminent companies with outstanding expertise in cyberspace and IT, world class higher education institutions, Fort Meade, federal and state agencies and other institutions, has the unique opportunity to be the leader in and epicenter of cybersecurity. Our state's current and future public safety and economic prosperity will depend on how we meet the challenges of securing and protecting our important databases and advancing cyber innovation and jobs. Instead of waiting for Congress, the Commission has propelled Maryland forward in passing significant legislation to protect its citizens against serious cyber attacks and formulating strategies for advancing cyber innovations and jobs that will allow the state to compete globally and sustain our future. While the Commission has made significant progress, there is still critical work ahead. As its important task has only begun, the Commission must be allowed to build on the momentum and gains made and continue its vital work in making Maryland the epicenter of cybersecurity.

IX. Appendix

Final Reports

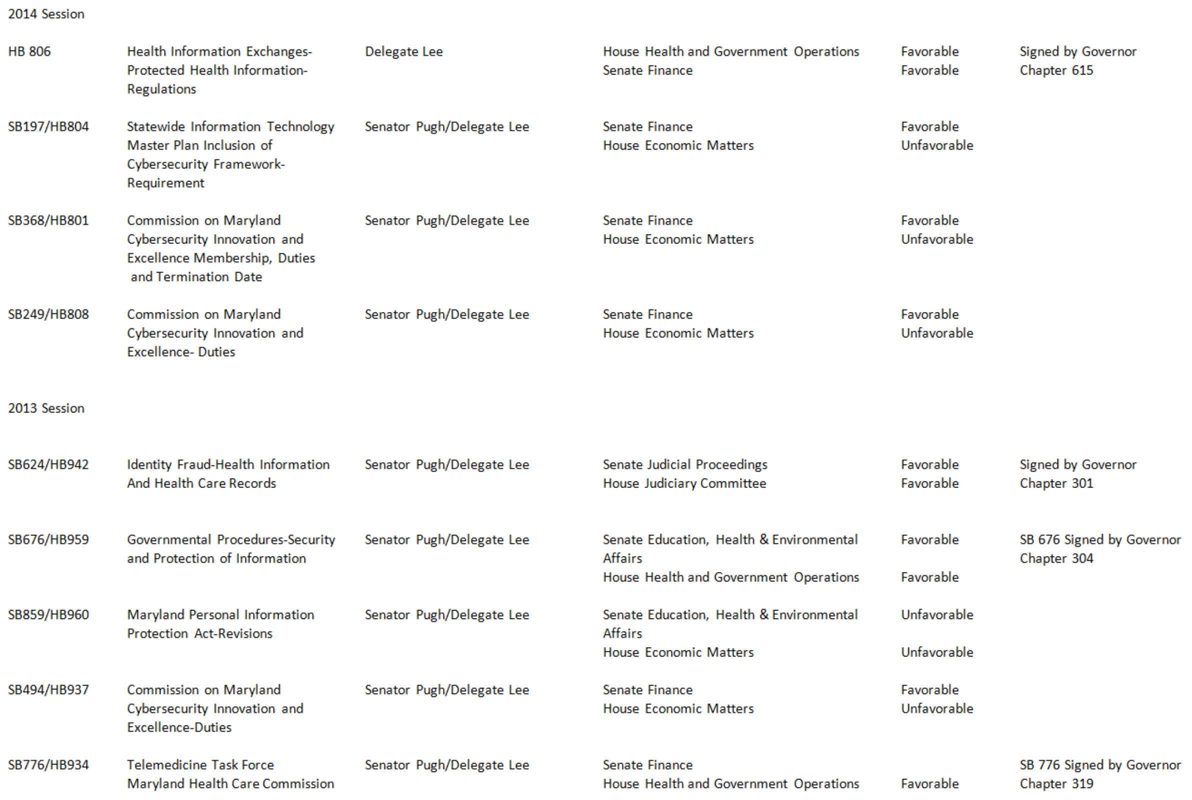
of

Commission Subcommittees

Commission on Maryland Cybersecurity Innovation & Excellence

Legal Strategy Subcommittee

Final Report



2014 Session					
HB 806	Health Information Exchanges-Protected Health Information-Regulations	Delegate Lee	House Health and Government Operations Senate Finance	Favorable Favorable	Signed by Governor Chapter 615
SB197/HB804	Statewide Information Technology Master Plan Inclusion of Cybersecurity Framework-Requirement	Senator Pugh/Delegate Lee	Senate Finance House Economic Matters	Favorable Unfavorable	
SB368/HB801	Commission on Maryland Cybersecurity Innovation and Excellence Membership, Duties and Termination Date	Senator Pugh/Delegate Lee	Senate Finance House Economic Matters	Favorable Unfavorable	
SB249/HB808	Commission on Maryland Cybersecurity Innovation and Excellence- Duties	Senator Pugh/Delegate Lee	Senate Finance House Economic Matters	Favorable Unfavorable	
2013 Session					
SB624/HB942	Identity Fraud-Health Information And Health Care Records	Senator Pugh/Delegate Lee	Senate Judicial Proceedings House Judiciary Committee	Favorable Favorable	Signed by Governor Chapter 301
SB676/HB959	Governmental Procedures-Security and Protection of Information	Senator Pugh/Delegate Lee	Senate Education, Health & Environmental Affairs House Health and Government Operations	Favorable Favorable	SB 676 Signed by Governor Chapter 304
SB859/HB960	Maryland Personal Information Protection Act-Revisions	Senator Pugh/Delegate Lee	Senate Education, Health & Environmental Affairs House Economic Matters	Unfavorable Unfavorable	
SB494/HB937	Commission on Maryland Cybersecurity Innovation and Excellence-Duties	Senator Pugh/Delegate Lee	Senate Finance House Economic Matters	Favorable Unfavorable	
SB776/HB934	Telemedicine Task Force Maryland Health Care Commission	Senator Pugh/Delegate Lee	Senate Finance House Health and Government Operations	Favorable	SB 776 Signed by Governor Chapter 319

The Legal Strategy Subcommittee of the Commission on Maryland Cybersecurity Innovation and Excellence introduced two (2) breach notification bills in the 2013 Session of the Maryland General Assembly to protect the individuals and their personal information: (1) SB 859/HB 960- Maryland Personal Information Protection Act-Revisions, which addressed requirements for businesses for breach notification; and (2) SB 676/ HB 959-Governmental Procedures-Security Protection of Information, which applied to certain governmental entities.

HB 859/ HB 960 did not move forward as it received an unfavorable report from the House Economic Matters Committee. SB 676 cross filed with HB 959 received favorable reports from the House Health and Government Operations Committee and the Senate Education, Health and Environmental Affairs Committee, passed the General Assembly and was signed by the Governor Martin O'Malley on May 2, 2013.

Both bills addressed breach notification requirements applicable for businesses and the state government. They required the appropriate entities to notify individuals of a breach of unencrypted personal information. A breach is the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information.[1] As a result, businesses must continue to comply with the existing breach notification law applicable to commercial entities, and certain governmental units now are required to adhere to standards similar to what the businesses must follow.

SB 959/HB 960, which applied to businesses, received an unfavorable report by the Economic Matters Committee and, thus, did not pass the legislature. Some businesses opposed the bill because it heightened existing standards regarding the protection of personal information. Businesses were concerned, for example, that the definition of "personal information" was too broad and that the legislation would create an additional financial burden. Thus, the standards of the existing breach notification law remain the same.

SB 676 cross filed with HB 959 passed the General Assembly, was signed by Governor Martin O'Malley on May 2, 2013, and went into effect on July 1, 2014. The law sets forth provisions for protecting citizens' personal information held by state government agencies (including local government units) and notification requirements when there is a breach. The judicial and legislative branches which were deleted from the bill out of concerns expressed by those branches that the judiciary and legislative branches have unique issues and challenges in protecting their data, including the costs involved. There was discussion about future legislation more tailored to each governmental branch.

Now that some Maryland governmental units are required to notify of a security breach involving personal information, Maryland is no longer far behind other states that have enacted breach notification legislation applicable to governmental units. The Legal Strategy Subcommittee is committed to making further progress in the next legislative sessions to continue to protect the state and individuals from cyber attacks and crimes.

In addition to this law, the General Assembly and the Governor signed SB 624/ HB 942- Identity Fraud- Health Information and Health Care Records (a bill on medical identity fraud). SB 494/ HB 937 –Commission on Maryland Cybersecurity Innovation and Excellence – Duties (a telemedicine related bill) received an unfavorable report by the House Economic Matters Committee and did not move forward.

SB 624/ HB 942 expand the identity fraud statute to include "health information" and "health care." Protected health information (PHI) has become valuable information for those wanting to commit criminal acts. Criminalizing this conduct now allows prosecutors to prosecute these

[1] Per Maryland legislation, "personal information" means "an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

1) a Social Security number;
2) a driver's license number, state identification card number, or other individual identification number issued by a [governmental] unit;
3) a passport number or other identification number issued by the United States Government;
4) an Individual Taxpayer Identification Number; or
5) a financial or other account number, credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account."

offenses of fraudulent use or possession of PHI, as well as to allow victims of this conduct to seek restitution. Under the law, a person may not:

A. Knowingly, willfully, and with fraudulent intent possess, obtain, or help another person to possess or obtain any personal identifying information of an individual, without the consent of the individual, in order to access health information or health care in the name of the individual;
B. Knowingly and willfully assume the identity of another person, including a fictitious person, with fraudulent intent to access health information or health care; and
C. Knowingly, willfully, and with fraudulent intent use a re-encoder or a skimming device to engage in specified activities in order to access health information or health care.

SB 494/HB 937 required the Commission to study and develop specified strategies and recommendations for advancing telemedicine technologies and use, including (1) methods of supporting innovation, development, and investment in the emerging technology; (2) the role of telemedicine in reducing health care disparities and addressing primary care and specialty care provider shortages across the continuum of care; (3) the protection of databases in the use of telemedicine; and (4) any other issue related to advancing and supporting telemedicine technologies and use. This bill did not move forward after receiving an unfavorable report from the House Economic Matters Committee.

The Legal Strategy Subcommittee of the Maryland Commission on Cybersecurity Innovation & Excellence is chaired by Michael Greenberger, JD.

Commission on Maryland Cybersecurity Innovation & Excellence

State Structure and Best Practices Subcommittee

Final Report

The Commission on Maryland Cybersecurity Innovation and Excellence Subcommittee on State Structure and Best Practices met periodically, including a working session to review the many resources, programs, best practices, and opportunities that already exist in Maryland and the US Federal Government that might be leveraged by state agencies. To formulate findings and recommendations, the Subcommittee aligned state priorities with national priorities for critical infrastructure security and resilience; reviewed means for leveraging relevant national programs, initiatives, and standards, and reviewed applicable performance audit reports of the Department of Information Technology and selected State agencies.

SUBCOMMITTEE MEMBERS

Barbara Gonzalez (Pepco Holdings, Inc.)
Joe Jarzombek (Department of Homeland Security Office of Cyber security & Communications)
Russell Butler (Maryland Crime Victims)
Frederick Ferrer (MCAC, Cyberspace ARINC)
Rob Rosenbaum (Maryland Tedco)
Betsy Hight (Hewlett-Packard)

VISION

Maryland state agencies protect interests of citizens by securing critical cyber infrastructure that operates services and stores/transmits data relevant to residents and organizations. The Maryland government and industry within the State that operates critical infrastructure prioritize cybersecurity and resilience as key to mission and business fulfillment.

MISSION

Review current structure and practices within the State Agencies in order to achieve the Governor's vision for the state's cybersecurity future, and make recommendations, as appropriate.

AREAS OF FOCUS

Priorities aligned with Citizen Protection, Privacy, Operational Support, and Law Enforcement:

- Financial (Accounting and receivables: payroll, taxes, social services benefits, etc.)
- Privacy (Health records, social services, motor vehicle administration, social security)
- Public Safety (criminal justice records, emergency management, etc.)

Current Conditions:

- Cyber standards implemented by all the agencies to meet or exceed security requirements
- Management Structure with cyber responsibilities, funding and resources to mitigate risks attributable to cyber attacks (Financial, Health Care, Social Services, Public Safety, etc.)

- Public Education & Transparency and Awareness

Future Conditions:

- Identify the gaps between the current state and the long term vision
- Develop a plan of action (organization, resources, standards, operating practices, priorities, etc.) with targets to be achieved

RECOMMENDATIONS

1. DoIT and State agencies should provide an update progress report in response to the Findings and Recommendations of the September 2012 Performance Audit focused on:

- Objective 1: State Law and DoIT Policies (State Law Requirements and DoIT Information Security Policy)
- Objective 2: Selected State Agency Security Practices (Compliance with DoIT Security Policy Requirements Inventory of Information Systems and Incident Response Process

For the most part, with the exception of Finding #2, DoIT and the State agencies agreed with the findings and recommendations of the September 2012 Performance Audit Report and indicated how the deficiencies would be addressed. However, with the exception of security awareness training being provided to all employees and being tracked, it is not readily apparent to what extent DoIT and State agencies are following-up in response to the performance audit recommendations.

- As a minimum, for each of the 12 findings, DoIT and/or the respective State agencies should provide an update on implementation status with respective timelines for the associated remedies, or justifications as to why full implementation has yet to be realized.
- The update progress report should include details about how DoIT and State agencies are monitoring and tracking performance relative to the NIST Cybersecurity Framework and the Critical Infrastructure Cyber Community (C3) Voluntary Program.
- As part of that update, DoIT and each State Agency should specify which NIST 800-53 rev4 security controls are used; indicating how selected controls address priorities aligned with citizen protection, privacy, operational support (and mission continuity), and, as applicable, law enforcement.

2. The Chief Information Security Officer (CISO) should have an independent reporting path to top State leadership, independent of the Chief Information Officer (CIO), to provide status updates and advise on the cyber resilience of Maryland's IT infrastructure.

3. DoIT should establish a comprehensive State-wide Incident Response Process and Capability, initially under the CISO for the State. While DoIT and each State agency will have incident response capabilities, it is important to understand that no single organizational entity would have the capability to adequately address the growing threat associated with cyber attacks. Information sharing for threat analysis and incident management is needed among State organizations, in coordination with industry and US Government departments and agencies.

4. DoIT, in coordination with industry, should establish a program for developing the capability to track and report on the cyber resilience of Maryland's critical infrastructure,

including all State agencies. This should be done consistent with the Critical Infrastructure Cyber Community (C3) Voluntary Program that uses a unified approach to cyber risk management for critical infrastructure sectors, and this includes State agencies and industry that operates infrastructure upon which citizens rely for critical services. The approach organizes Cybersecurity Framework-related awareness and engagement based on the priority risks to each sector.

The Subcommittee commends the State Legislature for passing bills during the tenure of this Commission that will better enable State agencies and industry to secure their part of cyberspace.

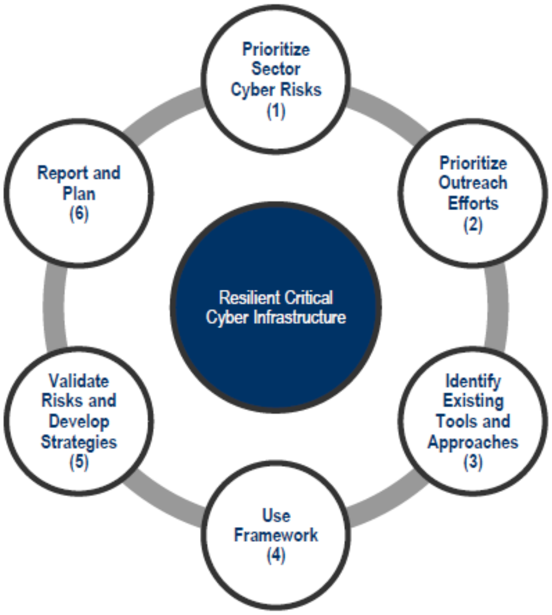
BACKGROUND

The Subcommittee met periodically to review the many resources, programs, best practices, and opportunities that already exist and are evolving in Maryland and the US Federal Government that might be leveraged by DoIT, State agencies, and those operating Maryland's critical infrastructure upon which citizens rely for services. The Subcommittee deliberated on State-level security topics for consideration:

1. Security vs. Compliance, how much should organizations deal with compliance, if at all?
2. To what State function should a State CISO report?
3. Policy and Enforcement vs. Guideline and Support vs. hybrid approach:
    a. Hybrid Option for "guide" until state organization "proves" help is needed (based upon some metrics), then policy and enforcement
    b. Hybrid Option to default "guide" except for "high risk" organizations where policy and enforcement would be applied
4. Monitoring component included or existing audit augmentation or any audit function?
5. Central Services vs. distributed services vs. hybrid approach (e.g. centralize costly "commodity based" services (e.g. Secure Operations Center), but leave unique (e.g. application) security to owning organization)
6. Critical Infrastructure definition and support
7. Privacy component(s)
8. Business Continuity (including "ruggedness"/resiliency)
9. Leverage proven and "non-technical" Best Practice Model for organizational measurement and roadmap to organizational security

The Subcommittee members realized that many models, frameworks and standards are available to guide process improvement and assess cyber security capabilities; yet each sector and agency has a different set of mission and business priorities. Indeed DoIT and State agencies have continued to use NIST Special Publications relevant to information security.

The Critical Infrastructure Cyber Community (C3) Voluntary Program, administered and coordinated by the US Department of Homeland Security Office of Cybersecurity and Communications, has introduced a unified approach to cyber risk management to the critical infrastructure sectors, and this includes State agencies and industry that operates infrastructure upon which citizens rely for critical services.


Prioritize Sector Cyber Risks (1)
Prioritize Outreach Efforts (2)
Identify Existing Tools and Approaches (3)
Use Framework (4)
Validate Risks and Develop Strategies (5)
Report and Plan (6)
Resilient Critical Cyber Infrastructure

The C3 Voluntary Program approach organizes Cybersecurity Framework-related awareness and engagement based on the priority risks to each sector. Accounting for unique sector needs and operating environments, the approach promotes existing sector cyber risk efforts underway, and leverages perspectives from companies using the Framework to validate sector risk priorities and inform corresponding sector-wide cyber risk management strategies. The C3 Voluntary Program developed the unified approach in response to Presidential Executive Order 13636 and Presidential Policy Directive 21, building on previous efforts to increase the cyber resilience of critical infrastructure. The diagram represents the approach. While the approach includes a series of six steps, agencies or sectors may either conduct steps independently based on what is most appropriate for their needs, or complete all six steps in a sequence. Government and industry can lead the approach in collaboration. This approach allows Sector-Specific Agencies (SSA) to align distinct cyber risk activities occurring in their sectors to broader cybersecurity resilience goals at state and national levels. SSAs can also use the approach to form strong sector partnerships, sector cyber risk management strategies, and risk-informed Sector-Specific Plans (SSP). The C3 Voluntary Program can help each organization or sector tailor it to sector environments. In partnership with the SSAs, the C3 Voluntary Program is also reaching out to sector members for their perspectives on sector cyber risk management efforts. For more information on the C3 Voluntary Program, see www.dhs.gov/ccubedvp and www.us-cert.gov/ccubedvp.

The Subcommittee on State Structure and Best Practices conducted an in-depth working session on 16 Jan 2013 to review the many resources, programs, best practices, and opportunities that already exist and are evolving in Maryland and the US Federal Government that might be leveraged by State agencies. It reviewed the Cybersecurity Findings and Trends in States, as reported by Deloitte and Touche, and discussed considerations for what is needed and why. The subcommittee reviewed NIST and Federal Government risk management guidance and reviewed options for guiding process improvement and benchmarking organizational capabilities that included several frameworks and models. Contracting for IT capabilities with cybersecurity perspective continues to be a critical issue because of external dependencies resulting from the increased reliance on suppliers of IT products and services. The session ended with considerations for both State Agencies and critical infrastructure within the State. It was agreed that while the focus has been on structuring recommendations for State agencies, much of this should have implications for critical infrastructure upon which citizens rely for services.

One of the key concerns raised in the Jan 2013 session was the September 2012 Performance Audit on the Department of Information Technology and Selected State Agencies in the report provided by the Office of Legislative Audits, Department of Legislative Services, Maryland General Assembly. Focused on Information System Data Security, the findings indicated:

- Department of Information Technology Needs to Develop a Process to Monitor and Enforce the Provisions of its Information Security Policy
- State Agencies Should Comply With the Provisions of the Information Security Policy to Help Ensure the Protection of Confidential Information

The Findings and Recommendations of the Performance Audit focused on:

- Objective 1: State Law and DoIT Policies (State Law Requirements and DoIT Information Security Policy)
- Objective 2: Selected State Agency Security Practices (Compliance with DoIT Security Policy Requirements Inventory of Information Systems and Incident Response Process)

For the most part, with the exception of Finding #2, DoIT and the State agencies agreed with the Performance Audit Findings and Recommendations; indicating how the deficiencies would be addressed. However, with the exception of security awareness training being provided to all employees and being tracked, it is not readily apparent to what extent DoIT and State agencies are following-up in response to the performance audit recommendations.

Finding 1 – Current State Law Governing Certain Protections for Personal Identifiable Information Did Not Apply to State Agencies

Finding 2 – DoIT Did Not Have a Formal Process in Place to Enforce the Provisions of its Information Security Policy

Finding 3 – DoIT Could Improve Guidance to Help Agencies Address Certain Security Issues

Finding 4 – DoIT Needs to Develop a More Responsive Process to Address Emerging Technologies and a Policy Regarding Mobile Devices

Finding 5 – DoIT Had Not Developed Recommended Practices for Implementing Data Loss Prevention Solutions

Finding 6 – State Agencies Often Did Not Document the Security Categorization of Information Systems

Finding 7 – Certain Agencies' Information Security Policies Were Not Agency Specific or Did Not Include All Required Components

Finding 8 – Risk Management Processes Were Not Fully Implemented

Finding 9 –Security Awareness Training Was Not Always Provided to Employees or Tracked

Finding 10 –Data Contained on Portable Devices Was Not Always Properly Protected Use of Certain Information Security Best Practices

Finding 11 – State Agencies Were in Various Stages of Implementing Data Loss Prevention Tools and Techniques

Finding 12 – State Agencies Had Varied Practices in Implementing Vulnerability Scanning and Penetration Testing

For Finding 2 – DoIT agreed that additional monitoring and enforcement of agency compliance with the Policy would be beneficial. The responsibility for compliance, monitoring, and enforcement tasks are currently delegated to agencies. The example within the recommendation models the Federal approach. DoIT agreed this approach could be used to formalize DoIT's monitoring and enforcement process. This would require additional resources/ investments in software and staffing to manage reporting, analyze results, and develop recommendations. Until such time as DoIT has these resources, the current policy of delegating to the agencies is deemed the most appropriate way to ensure compliance with State security policy and will remain in effect. NOTE: The DoIT response to the Performance Audit Report Finding 2 was generated before the national release of the Cybersecurity Framework and the C3 Voluntary Program.

With the exception of security awareness training being provided to all employees and being tracked, it is not readily apparent to what extent DoIT and State agencies are following-up in response to the performance audit recommendations. As such, the Subcommittee recommends:

- As a minimum, for each of the 12 findings, DoIT and/or the respective State agencies should provide an update on implementation status with respective timelines for the associated remedies, or justifications as to why full implementation has yet to be realized.
- The update progress report should include details about how DoIT and State agencies are monitoring and tracking performance relative to the NIST Cybersecurity Framework and the C3 Voluntary Program.
- As part of that update, DoIT and each State Agency should specify which NIST 800-53 rev4 security controls are used; indicating how selected controls address priorities aligned with citizen protection, privacy, operational support (and mission continuity), and, as applicable, law enforcement.

Commission on Maryland Cybersecurity Innovation and Excellence

Subcommittee on Education and Training

Final Report

The Commission on Maryland Cybersecurity Innovation and Excellence Subcommittee on Education and Training met regularly over the past eighteen months. The Subcommittee created a vision for cybersecurity education and training in the state, looked at barriers to meeting the vision, and developed recommendations to move the state closer to realizing the vision. Along the way the Subcommittee learned about the many resources, programs, best practices, and opportunities that already exist in Maryland**.**

SUBCOMMITTEE MEMBERS

Christian Anthony (Johns Hopkins APL)
Chieh-san Cheng (Global Science & Technology, Inc)
Darrell Drust (Lockheed Martin)
Sean Fahey (Johns Hopkins APL)
Megan Ferguson (Knowledge Advantage Inc.**)**
Frederick Ferrer (Cyberspace ARINC)
Barbara Gonzalez (Pepco Holdings, Inc)
Rear Admiral Elizabeth (Betsy) A. Hight (USN, Ret.)
Joe Jarzombeck (Department of Homeland Security)
Kelly Koermer (Anne Arundel Community College)
Kent Malwitz (UMBC)
Kathy Michaelian, Chair (Montgomery College)
Pat Mikos (Maryland State Department of Education)
Casey O'Brien (National CyberWatch Center, Prince George's Community College)
Joseph Whittaker (Morgan State University)

VISION

Maryland citizens will be afforded the opportunity to have the skills they need aligned to the career opportunities in cybersecurity and personal use of services delivered in cyberspace through abundant, diverse, and affordable education and training programs. The cybersecurity industry and government entities will recognize and employ this talented, qualified pool of workers to support cybersecurity innovation in the State.

BARRIERS

Institutional

- State higher education institutions have programs that do not always complement, and sometimes "compete" with, one another.
    - Difficulties articulating Computer Science and Cybersecurity programs between community colleges and 4-year institutions.
- Tremendous need for exceptional, experienced, and innovative teachers and faculty—where/how do we rank in having the "best and brightest" in the STEM and Cyber fields.

    - Shortage of qualified Computer Science and Cybersecurity teachers, especially at the high school level.
    - Difficulty finding a pool of qualified Cybersecurity faculty at the community colleges.
- High school curriculum does not offer the broadest exposure to either Computer Science or Cybersecurity. Only 61% of Maryland high schools offer Computer Science courses and less than half of all high schools offer more advanced Computer Science or programming courses.
- Lack of agility in the college and university Computer Science programs.
    - Software assurance needs to be included in the curriculum and often isn't. Challenge with finding room in an already packed curriculum.
    - Need for flexibility and speed for introducing and teaching new programming languages.

Population – this is really the biggest barrier – there is a small pool of interested and prepared students at the beginning of the pipeline.

- The existing (current) pool of students in Maryland does not have the STEM/Computer Science education and skills necessary to become the critical cyber workforce needed for the future.
- Not enough people are programming – need to attract and excite people into the field early.
- Still no real hook to incentivizing young people to take on STEM-related fields of study—no coolness or "Space Race" mentality.

Political/Legislative

- Aside from rhetoric and posturing, key leaders must really be proactive in promoting STEM/Computer Science in the high schools and helping universities and colleges fund and build necessary curricula and infrastructure. Need to build better bridges and transitions between high schools and colleges.
- Lack of State-level marketing and positioning state educational institutions as the nation's premier cyber technology leaders.
- State and federal contracts are written that require 4-year degrees when many jobs could be filled by qualified community college students.

RECOMMENDATIONS

Growing the Pipeline K-12 (It is the Subcommittee's belief that the most effective and sustainable solution to address this crisis is to try to get as many kids exposed to high quality computer science education as early as possible. If there are large numbers of well-prepared CS students flowing into the community colleges and 4 year institutions, a certain percentage of these will be attracted to the field of cybersecurity).

- Provide funding to support the creation of Computer Science Certification programs in Maryland Colleges and Universities to facilitate the adequate preparation and credentialing of high school computer science teachers. Provide funding to support students interested in taking this program.

- Incentivize the process to get more current teachers in Maryland's secondary schools certified in Computer Science and Cybersecurity. Incentives could be financial or otherwise (sabbaticals, externships, use of community college classes to meet certification requirements, etc.).
- Offer "Exploring Computer Science" at the middle school level, where possible.
- Include Computer Science and Cybersecurity courses as options for students for the required MSDE Technology Education credit for high school graduation. Promote offering "Exploring Computer Science" or "Computer Science Principles" in all Maryland high schools. This will require recruitment and incentives for having a qualified CS teacher at every school or at least available to the school.
- Expand ongoing cyber-awareness (including cyber ethics and cyber safety) activities and requirements in K-12, leverage existing resources by looking at and replicating best practices across the state.
- Expand MD Virtual Online offerings. Offerings are currently limited to an AP Computer Science A and an Oracle 3 database course. New Computer Science and Cybersecurity courses are under development and will be available starting in the 2014-2015 school year.
- Expand co-curricular programs and transformative types of activities.
- Develop online cyber education for Maryland K-12 students.
- Leverage and support the NSF-funded CE21 initiative (http://ce21maryland.umbc.edu/). In year 3 of this grant, which is when the professional development of "in service" teachers (teaching existing teachers how to effectively teach CS) is being rolled out regionally; funding and other support will be needed by each region. Additional, external funding would allow more teachers to be trained and sooner.

Academic Innovation and Collaboration

- Provide encouragement, resources and institutional funding that will:
  - lead to all of Maryland's educational institutions (K-16) with Cybersecurity related programs mapping outcomes to common standards.
  - lead to smooth statewide articulations between high schools, community colleges, and four-year school programs (2+2+2).
  - incentivize the creation of curriculum and expansion at selected USM schools that articulates with the community college Cybersecurity AAS curriculum to provide pathways to bachelor's degree for students. Programs that articulate already exist at Bowie State University, Capitol College, and UMUC.
  - assure that community colleges and universities incorporate software assurance concepts into their Computer Science curricula.
  - develop academic pathways and bridge programs for students changing their educational focus.
  - incorporate cyber related concepts across the curriculum (for example in business, psychology, and ethics).

Pathways to Employment

- Create and support multiple pathways to job roles (not just necessarily the bachelor's degree).

- Through example at the State level, influence the corporate culture that requires a bachelor’s degree. Encourage portfolio review (military/work experience, industry certifications, etc.) as a substitute for degree attainment alone.

Partner with Industry for Innovative Ways to Support Student Learning

- Involve industry in teacher exchanges, externships, mentorships (for both students and teachers).
- Empower industry practitioners in the classroom.
- Expand co-curricular programs and transformative type of activities involving industry. For example, afterschool programs, field trips, clubs, and competitions.
- Incentivize businesses to take student interns.
- Use the existing Maryland Business Roundtable to create a sub-group focused on cybersecurity and computer science.

Marketing and Dissemination

- Develop a clearinghouse that includes regularly updated environmental and curricula scans. Look at the possibility of expanding existing resource centers like the National CyberWatch Center Clearinghouse or CyberMaryland. There is a ton of good stuff going on in Maryland and no centralized place to gather and disseminate information.
- Develop a marketing plan highlighting what Maryland’s educational institutions have already achieved. For example, the number of institutions recognized as National Centers of Academic Excellence in Information Assurance (tied with Texas for the most - 16) and the largest concentration of National Centers of Academic Excellence in Information Assurance 2-Year Education (eight in state).