Maryland Cybersecurity Council

Initial Activities Report

July 1, 2016

Introduction

The integrity of Maryland's operational infrastructure is tied to our commitment to protect it. A major cyber attack against any of Maryland's critical infrastructure could have catastrophic consequences to the State's economy, vital services, and the health and safety of its citizens. It is therefore of the utmost importance that we protect the State's critical infrastructure—including electric power grids, transportation systems, financial systems, and communication networks—as well as the data that has been entrusted to the State by its citizens.

A review of the cybersecurity industry in Maryland reveals that Maryland has the necessary elements for becoming the nation's cybersecurity leader. Some of the major federal agencies with cybersecurity as their principal mission are headquartered in Maryland. There is a strong and dedicated industry around these major installations to support their cybersecurity mission. Maryland's academic institutions have been highly successful in responding to the workforce demands of the cyber industry, offering cybersecurity skills training and incubators for new and growing businesses. Together, these entities have created an excellent ecosystem for cybersecurity innovation and job growth in Maryland. Given that Maryland has these strengths in cybersecurity, it should increase its efforts to enhance its cybersecurity posture and expand innovation and job growth.

In 2015 the Maryland General Assembly created, through Senate Bill 542, the Maryland Cybersecurity Council to develop comprehensive strategies and recommendations to protect the State's critical infrastructure and move Maryland forward as a hub of cybersecurity innovation and jobs. The Council brought together stakeholders that include members of the General Assembly, State agencies, law enforcement, higher education institutions, businesses, the healthcare sector and other organizations susceptible to cyber attacks.

To achieve its mission and purpose, the Council established subcommittees around six main areas: law, policy and legislation; cyber operations and incident response; critical infrastructure and cybersecurity framework; education and workforce development; economic development; and public awareness and community outreach. The Council held three full Council meetings and numerous subcommittee meetings during its first year. In February, the Council welcomed Google Vice President Dr. Vincent Cerf, who discussed the evolution of the internet and stressed the importance of increasing government enforcement of internet security measures. Based on its observations and discussions, the Council in this initial report makes several recommendations to protect the State's critical infrastructure and enhance the State's economic growth. Implementing these recommendations will help the State strengthen its critical infrastructure and advance its leadership in cybersecurity innovation.

Table of Contents

I. Background

The Maryland Cybersecurity Council was established by Senate Bill 542 during the 2015 legislative session. The purpose of the Council is to form strategies and recommendations for protecting the State's critical infrastructure while advancing cyber innovation and jobs in Maryland. The Council will work with relevant entities towards accomplishing the critical task of assessing and improving the State's cybersecurity posture.

II. Council Membership

Under the leadership of Attorney General Brian Frosh, serving as Chair, the Council brings together stakeholders that include, members of the General Assembly, State agencies, law enforcement, higher education institutions, business, cyber technology representatives, healthcare, trade, and other organizations susceptible to cyber attacks. The Council members are as follows:

Chair: Brian E. Frosh, Maryland Attorney General

Legislative Representatives:

- Susan C. Lee, Senator, Maryland General Assembly
- Catherine E. Pugh, Senator, Maryland General Assembly
- Ned Carey, Delegate, Maryland General Assembly
- Mary Ann Lisanti, Delegate, Maryland General Assembly

Technology Companies:

- Belkis Leong-Hong, Founder, President, and CEO, Knowledge Advantage, Inc.
- Rajan Natarajan, PhD, President, TechnoGen, Inc.
- Jonathan Powell, Senior Program Manager, CACI, Inc.
- Zuly Gonzalez, Co-Founder and CEO, Lightpoint Security
- James Foster, CEO, ZeroFox
- John M. Abeles, President and CEO, System 1, Inc.

Business Associations:

- Don Fry, President and CEO, Greater Baltimore Committee
- Joseph Morales, JD, Attorney, Maryland Hispanic Chamber of Commerce
- Jim Dinegar, President and CEO, Greater Washington Board of Trade
- Brian Israel, Business Development Executive, Maryland Association of Certified Public Accountants

Higher Education:

- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland
- Jonathan Katz, PhD, Director, Maryland Cybersecurity Center and Professor, Department of Computer Science, University of Maryland, College Park
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Patrick O'Shea, PhD, Vice President and Chief Research Officer, University of Maryland, College Park
- Anton Dahbura, PhD, Executive Director, Information Security Institute, Johns Hopkins University
- Shiva Azadegan, PhD, Director, Computer Science, Towson University
- David Wilson, EdD, President, Morgan State University
- Carl Whitman, Vice President, Instructional and Information Technology and Chief Information Officer, Montgomery College
- David Anyiwo, PhD, Professor and Chair, Department of Management Information Systems, Bowie State University

Crime Victim Representative:

- Sue Rogan, Director, Financial Education, Maryland CASH Campaign

Susceptible Industries:

- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Clay House, Vice President, Architecture, Planning, and Security, CareFirst
- Pegeen Townsend, Vice President, Government Affairs, Medstar Health
- Jayfus Doswell, PhD, Founder, President, and CEO, The Juxtopia Group, Inc.
- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System

Other Designees:

- Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program Brookings Institution
- Howard Feldman, JD, Attorney, Whiteford, Taylor & Preston
- Paul Tiao, JD, Attorney, Hunton & Williams
- Robert W. Day Sr., Senior Security Monitoring Analyst, AECOM, Inc.
- Jonathan Prutow, Senior Associate, Aveshka, Inc.
- Larry Letow, President and CEO, Convergence Technology Consulting
- Mark Augenblick, JD, Attorney, Pillsbury Winthrop Shaw Pittman LLP
- Henry J. Muller, Director of Communications-Electronics Research, Development and Engineering Center, U.S. Army, Aberdeen Proving Ground

Federal Institutions:

- Judith Emmel, Associate Director, State, Local, and Community Relations, National Security Agency
- Donna Dodson, Director, National Cybersecurity Center of Excellence, National Institute of Standards and Technology

State Institutions:

- David Garcia, Secretary of Information Technology, Maryland Department of Information Technology
- Col. William Pallozzi, Secretary of State Police, Maryland State Police
- Ken McCreedy, Director, Cyber Development, Maryland Department of Commerce
- Major General (MG) Linda Singh, Adjutant General of Maryland, Maryland Military Department
- Walter London, Director, Governor's Office of Homeland Security
- David Engel, Director, Maryland Coordination and Analysis Center
- Russell Strickland, Director, Maryland Emergency Management Agency
- Henry Ahn, Program Manager, Technology Funding Programs, Maryland Technology Development Corp.
- Phil Schiff, CEO, Tech Council of Maryland
- Anthony Lisuzzo, Board Member, Army Alliance
- Steven Tiller, President, Fort Meade Alliance
- Sachin Bhatt, Assistant Attorney General, Office of the Maryland Attorney General

III. UMUC's Role

University of Maryland University College (UMUC) supports the Maryland Cybersecurity Council in several ways: planning and hosting Council meetings; bringing expert resources to support the Council's work; working with the Council members and their institutions to support the Council's efforts; and drafting Council reports. The Council is currently staffed by UMUC Professor, Dr. Amjad Ali.

IV. Council Structure

The Maryland Cybersecurity Council is organized into the following subcommittees:

Law, Policy and Legislation Subcommittee

Subcommittee Objectives

- Examine and identify inconsistencies and gaps between State and Federal laws regarding cybersecurity; recommend any new legislation needed to address identified inconsistencies/gaps
- Recommend any legislative changes considered necessary by the Council to address cybersecurity
- Review cybercrime statutes and make recommendations for improvements thereto

Subcommittee Members

- Co-Chair: Susan C. Lee, Senator, Maryland General Assembly
- Co-Chair: Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution
- Joseph Morales, JD, Attorney, Maryland Hispanic Chamber of Commerce
- Pegeen Townsend, Vice President, Government Affairs, Medstar Health
- Howard Feldman, JD, Attorney, Whiteford, Taylor & Preston
- Ned Carey, Delegate, Maryland General Assembly
- Jonathan Prutow, Senior Associate, Aveshka, Inc.
- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland
- Paul Tiao, JD, Attorney, Hunton & Williams

Cyber Operations and Incident Response Subcommittee

Subcommittee Objectives

- Recommend best practices for monitoring and assessing cyber threats and responding to cyber attacks or other security breaches thereto
- Create or enhance shared awareness of cyber vulnerabilities, threats, and incidents within the State
- Recommend best practices for developing comprehensive state strategic plan to ensure a coordinated and quickly adaptable response to and recovery from cyber attacks and incidents[1]

[1] Senate Bill 542 lists the development of a comprehensive state strategic cyber security plan among the deliverables for the Cybersecurity Council. Md. Ann. Code, St. Gov't Art. §9-2901 (J)(6). However, the Council understands that this effort – which includes the review and analysis of highly sensitive and confidential data – has already begun under the direction of the Maryland Department of Information Technology in coordination with other State agencies. The Council will review and/or advise the Department's efforts as appropriate.

- Serve as a resource for its expertise to all other subcommittees

Subcommittee Members

- Chair: David Garcia, Secretary of Information Technology, Maryland Department of Information Technology
- Mary Ann Lisanti, Delegate, Maryland General Assembly
- Walter London, Director, Governor's Office of Homeland Security
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Anthony Lisuzzo, Board Member, Army Alliance
- Robert W. Day Sr., Senior Security Monitoring Analyst, AECOM, Inc.
- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System
- Robert Smolek, Major, Maryland State Police
- Judith Emmel, Associate Director, State, Local, and Community Relations, National Security Agency

Critical Infrastructure and Cybersecurity Framework Subcommittee

Subcommittee Objectives

- For critical infrastructure not covered by Federal law or Executive Order 13636 of the President of the United States, identify best practices in conducting risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures
- Use Federal guidance to identify categories of critical infrastructure as critical cyber infrastructure if cyber attacks to the infrastructure could reasonably result in catastrophic consequences
- Assist infrastructure entities that are not covered by the Executive Order in complying with Federal cybersecurity guidance
- Assist private sector cybersecurity businesses in adopting, adapting, and implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework
- Assist State of Maryland government entities, as well as educational entities, in adopting, adapting, and implementing the NIST Cybersecurity Framework
- Recommend strategies for strengthening public and private partnerships necessary to secure the State’s critical information infrastructure

Subcommittee Members

- Chair: Michael Greenberger, Director, Center for Health and Homeland Security, University of Maryland
- John M. Abeles, President and CEO, System 1, Inc.

- Dr. David Anyiwo, Chair, Department of Management Information Systems, Bowie State University
- Mark Augenblick, Attorney, Pillsbury Winthrop Shaw Pittman LLP
- Donna Dodson, Director, NIST National Cybersecurity Center of Excellence, National Institute of Standards and Technology
- David Engel, Director, Maryland Coordination and Analysis Center
- Zuly Gonzalez, Co-Founder and CEO, Lightpoint Security
- Clay House, Vice President, Architecture, Planning, and Security, CareFirst
- Rajan Natarajan, President, TechnoGen, Inc.
- Major General (MG) Linda Singh, Adjutant General of Maryland, Maryland Military Department

Education and Workforce Development Subcommittee

Subcommittee Objectives

- Enhance and support cyber workforce training and education in Maryland, including:
  - Recommendations for enhancing student interest in pursuing cybersecurity education; recommendations to develop programs enticing or incentivizing students and professionals to enter cybersecurity field
  - Recommendations for attracting teachers and faculty qualified to teach cybersecurity courses in high school and beyond
  - Recommendations to develop and modify high school and higher education curriculum to enhance cybersecurity skills and talent; recommendations for developing fundamental skills necessary for cybersecurity students and professionals
- Promote cyber research and development (R&D) in higher education
  - Recommendations on funding for R&D
  - Recommendations on incentivizing R&D
  - Recommendations for collaborative R&D
- Recommendations on pathways to employment in cybersecurity field

Subcommittee Members

- Chair: Jonathan Katz, PhD, Director, Maryland Cybersecurity Center and Professor, Department of Computer Science, University of Maryland, College Park
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove
- Jonathan Powell, Senior Program Manager, CACI, Inc.
- Henry J. Muller, Director, Communications-Electronics Research, Development and Engineering Center, U.S. Army, Aberdeen Proving Ground
- Shiva Azadegan, PhD, Director, Computer Science, Towson University
- Russell Strickland, Director, Maryland Emergency Management Agency
- David Wilson, EdD, President, Morgan State University

Economic Development Subcommittee

Subcommittee Objectives

- Promote cyber innovation for economic development, attracting private sector investment and job creation in cybersecurity
- Recommend strategies for increasing cybersecurity research and development funding
- Promote cybersecurity entrepreneurship in Maryland
- Recommend strategies for attracting cybersecurity companies to Maryland
    - attract venture capital
    - valuable tax incentives

Subcommittee Members

- Chair: Belkis Leong-Hong, Founder, President, and CEO, Knowledge Advantage, Inc.
- Jim Dinegar, President and CEO, Greater Washington Board of Trade
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Ken McCreedy, Director, Cyber Development, Maryland Department of Commerce
- Phil Schiff, CEO, Tech Council of Maryland
- Brian Israel, Business Development Executive, Maryland Association of Certified Public Accountants
- Steven Tiller, President, Fort Meade Alliance
- Don Fry, President and CEO, Greater Baltimore Committee
- James Foster, CEO, ZeroFox
- Henry Ahn, Program Manager, Technology Funding Programs, Maryland Technology Development Corp.

Public Awareness and Community Outreach Subcommittee

Subcommittee Objectives

- Promote the Council's objectives; spread awareness of Council's cybersecurity efforts and activities
- Learn and assess cyber concerns of businesses, community and individuals so Council can offer information that is relevant, applicable and valued
- Create a depository of cybersecurity awareness information for all, including private and public sectors as well as individuals

Subcommittee Members

- Chair: Sue Rogan, Director, Financial Education, Maryland CASH Campaign
- Catherine E. Pugh, Senator, Maryland General Assembly
- Patrick O'Shea, PhD, Vice President and Chief Research Officer, University of Maryland, College Park

- Anton Dahbura, PhD, Executive Director, Information Security Institute
  Johns Hopkins University
- Carl Whitman, Vice President, Instructional and Information Technology and Chief Information Officer, Montgomery College
- Jayfus Doswell, PhD, Founder, President, and CEO, The Juxtopia Group, Inc.
- Larry Letow, President and CEO, Convergence Technology Consulting

V. Recommendations

Based on observations and discussions during its first year, the Maryland Cybersecurity Council makes the following preliminary recommendations aimed at protecting the State's critical infrastructure and advancing cyber innovation and jobs in Maryland:

Law, Policy and Legislation

1. Cyber First Responders Reserve

The Council recommends the creation of a cyber first responders reserve, where an appropriate state agency would coordinate with top cyber expert reservists in the event of a cyber emergency. The Maryland Emergency Management Agency (MEMA) appears to be the appropriate agency to lead and coordinate the proposed cyber first responder reserve.

The United States government recently created a digital service corps to facilitate the hiring of digital expertise that was previously difficult to hire. In addition, the federal government and the individual states have a national reserve that can be called upon in the event of a natural or other kind of disaster. Due to the growing threat cyber attacks pose to our welfare, Maryland should also have access to a reserve of digital expertise in the foreseeable event of a cyber emergency. Combining the two ideas (digital service corps and national reserve), Maryland should create a cyber first responders reserve in order to access a reserve of expertise in the event of a cyber emergency.

2. MPIPA Personal Information and Breach/Unauthorized Access Definitions & other Changes

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 and expanding certain provisions of the MPIPA.

The Council recommends a legislative proposal to expand the applicability of MPIPA's data breach notification requirement by redefining "personal information" to include more types of data that can be used to identify a person. The definition for "personal information" would include the following:

1. Email address or username, plus password or security question
2. Patterned genetic information
3. Unique biometric data

This would build upon proposed legislation SB 29 (2016), SB 548 (2015), SB 859 (2013) and HB 960 (2013) to impose additional requirements on a business to protect an individual's personal information, including the implementation of reasonable security procedures and practices to safeguard the personal information.

The Council also recommends creating another category of data termed "private information." This category of data will be reserved for data that requires the absolute highest level of security and safeguards. The Council will conduct further research to offer an appropriate definition.

Finally, the Council recommends amending MPIPA to broaden the definition of what constitutes a "breach" to include not only "unauthorized acquisition" but also "unauthorized access." This broader definition accounts for a security incident where the perpetrator does not acquire the data but, instead, modifies it.

Prior to submission, the Council will refine this legislative proposal, particularly defining what constitutes "private information."

3. Civil Cause of Action for Remote Intrusions

The Council recommends the creation of a civil cause of action for remote intrusions. This recommended legislative initiative would provide a private party the ability to pursue a claim against a person or entity that accessed the private party's personal information without authority. Federal law includes such a cause of action, as do several other states. As government resources for state and local computer hacking prosecutions are limited, this proposal would provide a civil remedy for private parties to redress instances of unauthorized access to systems. Furthermore, it would serve the public interest by holding parties responsible for their wrongful conduct in accessing systems without authority.

The Council will conduct further analysis of relevant federal laws and laws in other states and examine the general parameters of the cause of action before submitting the legislative proposal to the General Assembly for consideration.

4. Credit Freeze

The Council recommends that Maryland further incentivize the practice of freezing credit account generation to prevent the improper uses of electronic information to mimic financial identities and cause irreparable damage to identity theft victims of all ages. Children in Maryland may already, at no charge, have their credit frozen until they reach age 18 because their credit identities are particularly vulnerable. The Council believes that that this policy should be expanded beyond children and recommends a legislative vehicle to reduce the hurdles to freeze and thaw credit access when there has been a data breach notice. Moreover, it is recommended that the ability to freeze one's credit should be well advertised by relevant state government agencies and promoted as a reasonable special safeguard against the financial externalities of identity theft. The key parameters of this legislative proposal are as follows:

a. Prohibiting a consumer credit agency from charging a fee for a placement, temporary lift, or removal of a credit or security freeze when the consumer has been a victim of a data breach
b. Establishing a violation as an unfair or deceptive trade practice
c. While a credit freeze can be necessary to prevent an identity thief from exploiting access to personal information, the consumer should not have to pay the cost of lifting the freeze to be able to have access to credit for a legitimate purpose.
d. The legislative proposal would also detail the information that must be provided to a consumer in the event of a credit freeze.

5. NIST Cybersecurity Framework

The Council recommends that the Secretary of the Maryland Department of Information Technology consider the National Institute on Standards and Technology (NIST) Cybersecurity Framework and other relevant federal guidance and standards when developing or modifying the Statewide Information Technology Master Plan.

6. Maryland Data Breach Report

The Council recommends that the Office of the Attorney General issue a periodic report designed to highlight the preceding year's notable events and trends in data security. The report should be a summary or "snapshot" of data security activity and trends relevant to Marylanders to include: data breach statistics; legislative and judicial developments in the area of data security; and best practices for businesses on data breach prevention and response.

Cyber Operations and Incident Response

7. Integrated Cyber Approach for Mid-Atlantic Region

The Council recommends examining the idea of coordinating other states and government cybersecurity efforts across the mid-Atlantic region. Federal and state emergency management agencies are well acquainted with these types of collaborations. By way of example, the New England states, FEMA Region 1, have integrated some of their cybersecurity efforts and have even exercised as a group in the Department of Homeland Security cyber exercises. The Council will be seeking examples, best practices and general research to determine the feasibility of establishing an integrated approach across the Mid-Atlantic region.

Critical Infrastructure and Cybersecurity Framework

8. Establishment of Educational Infrastructure

The Council recommends the establishment of an educational infrastructure in Maryland that could educate owners and operators of the State's critical infrastructure and other stakeholders on cybersecurity matters. This educational infrastructure would provide resources to Maryland critical infrastructure sectors and other stakeholders in the State. These resources would be based on the latest cybersecurity trends, guidance, and best practices. Specific areas to be covered by the cyber education infrastructure may include:

- General cybersecurity awareness
- Information sharing through Information Sharing and Analysis Organizations
- Cybersecurity frameworks, including the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
- Critical infrastructure tools for cybersecurity
- Cyber risk-management
- Cyber workforce development and training
- Other subjects based on stakeholder demand and the latest cybersecurity developments

The primary objective of the educational infrastructure would be to establish a plan to raise awareness of the cybersecurity threat, as well as methods and tools to address that threat. The Council envisions a multi-channel approach to achieve this goal, to include:

- Lectures, workshops, and discussion groups on various cybersecurity topics
- An on-line repository of lectures and presentations and other resources, freely available 24/7
- Conferences that serve to highlight cybersecurity issues for critical infrastructure
- Input from academic institutions in the development of educational materials and academic programs

The Council believes that this proposed cyber education infrastructure would gain wide support. Use of the cyber educational resources would be voluntary. Furthermore, because there is great variance in cybersecurity awareness and capabilities among Maryland's private institutions, this cyber education infrastructure would be a valuable resource to all of Maryland's critical infrastructure sectors and other stakeholders regardless of their cybersecurity sophistication. Stakeholders should be able to use the cyber education infrastructure resources and tailor them to their specific needs. Finally, this recommendation is one that could be implemented quickly and be built on in the future to support the critical infrastructure serving Maryland.

9. Critical Infrastructure and Risk Assessments

Identification of Critical Infrastructure

The Council intends to identify the critical infrastructure sectors that are at risk of cyber attacks. Pursuant to the Annotated Code of Maryland, State Government Article, 9-2901(J)(1), the Council will work with the National Institute of Standards and Technology and other Federal agencies, private sector businesses, and private cybersecurity experts to try to determine which local infrastructure sectors are at the greatest risk of cyberattacks and need the most enhanced cybersecurity measures. Furthermore, federal guidance will be used to identify critical infrastructure where cyber damage or unauthorized cyber access to the infrastructure could reasonably result in catastrophic consequences.

The Council recognizes that the cyber risk to critical infrastructure sectors will vary depending on the threat actor, specific vulnerabilities associated with each sector, and the vector from which various potential public and private sector victims are attacked. The Federal civilian agencies tasked with cybersecurity and critical infrastructure protection focus primarily on six sectors:

- Banking/Finance
- Communications
- Energy
- Healthcare
- Information Technology
- Transportation

These sectors are critically important to Maryland as well. It is also important to note that each of these sectors is uniquely vulnerable and the threat environment is fluid.

The Council recommends that no critical infrastructure sector be examined independently. Many interdependencies exist between critical infrastructure components and an exploited vulnerability in one sector could have cascading repercussions throughout other sectors. For example, most sectors are dependent on the electric grid. Interdependencies exist not only between sectors, but also geographically. While Article 9-2901(J)(1) references “local” infrastructure sectors, the Council recommends that critical infrastructure is examined beyond State boundaries. Critical infrastructure, such as the electric grid, may span the mid-Atlantic region and even nation-wide. It is important to recognize the instances where infrastructure is not localized within the State, but is dependent on factors well beyond the State’s control. It may, however, be challenging to identify all interdependencies adequately. The Council, therefore, sees an important role for government as a facilitator that can bring parties together to highlight sector interdependencies.

Risk Assessments

After critical infrastructure sectors have been identified, any risk assessments ought to be performed pursuant to the most effective methods and general best practices. As part of its work over the next year, the Council intends to gather these methods, best practices, and other resources and make them available to stakeholders.[2]

A difficult challenge for conducting risk assessments on critical infrastructure rests on the fact that the majority of critical infrastructure is privately owned. Thus, an owner of that infrastructure now has the ability to ignore government mandates pertaining to risk mitigation. The Council is optimistic, however, that carefully crafted incentives can be used to enlist the private sector in needed risk mitigation. The State should, therefore, gather tools and outline steps and best practices in performing risk assessments and provide them to critical infrastructure owner and other stakeholders.

A recommended set of tools and "best practices" for infrastructure protection would include the use by critical infrastructure sectors of the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (the NIST Cybersecurity Framework). Use of this Framework is voluntary, but should be highly encouraged by government. NIST has also developed the "Guide for Conducting Risk Assessments" (SP 800-30), which is a highly valuable resource that critical infrastructure sectors may use. Private sector critical infrastructure owners should also be encouraged to make use of the Critical Infrastructure Cyber Community C^3 Voluntary Program that supports stakeholders in their use of the NIST Framework. Furthermore, the Council recognizes that some suppliers of critical infrastructure may be compelled to adhere to alternative frameworks such as HiTRUST and ISO.

The Federal Department of Homeland Security (DHS) has published general guidance on critical infrastructure security and vulnerability assessments. This information is a good starting point to inform any effort to perform comprehensive and effective risk assessments. Moreover, the following Federal government resources can support vulnerability assessments:

- DHS National Protection and Programs Directorate to inform on internal risk management processes and to provide technical assistance
- DHS Office of Cybersecurity and Communication and its Cyber Resilience Review (CRR) process. The goal of CRR is to understand and measure key cybersecurity capabilities and provide indicators on operational resilience and the ability to manage cyber risk
- Self-evaluation tools, such as those made available through the United States Computer Emergency Readiness Team
- Infrastructure Protection Report Series, available through the Homeland Security Information Network, that identify common vulnerabilities to critical infrastructure by sector and also identify security and preparedness best practices

[2] Senate Bill 542 also requires, for critical infrastructure not covered by federal law or the Executive Order, that the Council actually conduct risk assessments to determine which local infrastructure sectors are at the greatest risk of cyber attacks and need the most enhanced cybersecurity measures. SG §9-2901 (J)(1). Performing risk assessments, however, is a complicated and costly venture. Without funding, the Council cannot meet this mandate. The Council will focus its efforts on identifying best practices for performing risk assessments of critical infrastructure.

- Training opportunities that include courses on critical infrastructure protection and security

Education and Workforce Development

10. Basic Computer Science and Cybersecurity Education

The Council recommends that the State expand its efforts to develop a pipeline of students interested in cybersecurity by exposing students to computer science in general, and cybersecurity principles in particular, at an early age. It is unacceptable that in 2016 students are required to learn physics, chemistry, and mathematics in high school, but there are still no requirements in place for computer science.

Although cybersecurity is a broad and multidisciplinary field, it is inextricably linked with computer-science education. The State should mandate a basic level of computer-science education for all. The State should also encourage the development of curricula for computer-science education at the middle-and high-school levels, including basic cybersecurity principles. This could be done via a state-federal partnership, in consultation with industry and academia, and by getting the State's P-20 Council to focus on this issue.

Other ways to encourage middle-and high-school students to learn about cybersecurity could include State-sponsored contests focusing not only on attacks, but also on foundational principles for building secure systems in the first place. The Build-it/Break-it/Fix-it context run by University of Maryland can serve as one possible model for this. Another possibility is to run summer camps such as the GenCyber camps run jointly by the National Security Agency and National Science Foundation in numerous states around the Country. In addition, the State could encourage mentorship opportunities with local industry or State government.

It is a challenge to find enough qualified teachers who can teach computer science at the middle- and high-school level. In the long term this problem can only be addressed by increasing the number of bachelor's degrees, and/or minors, awarded in computer science. In the near term this could be addressed by training current teachers who would be interested in transitioning to the subject, as is done as part of the GenCyber camps mentioned above. The State should also explore training retired computer science professionals to teach, and the Maryland State Department of Education should consider adding an M-CERT certification in computer science at the middle-school level.

11. Maryland Cyber Scholarship for Service

Focusing on the transition between high school and college, the Council recommends that the State enhance incentives for the top students interested in computer science and/or cybersecurity to remain in the State by providing scholarships to those students to attend schools in Maryland. The State may also want to consider a "scholarship for service" model at the State level, through which the State would pay for students' tuition and in return those students would work in State or local government for some number of years after graduation.

12. Resources for Computer Science Departments

Sufficient resources must be provided to computer-science departments within the University System of Maryland to ensure they can adequately meet student demand. Currently, demand is far outstripping the available capacity. For example, the University of Maryland, College Park, currently has over 2700 undergraduate computer science majors, a growth of about 150% over the last 5 years. If computer science and cybersecurity are to be a priority for the state of Maryland, sufficient resources must be dedicated within public universities to handle this level of interest.

13. Study of Cyber Workforce Demand and Skills

The term "cybersecurity education" is currently used to mean too many different things, both by educators and by industry, including encompassing very technical skills like penetration testing or reverse engineering to less specialized work in system administration or network management, and even extending to skills in related fields like cybersecurity law. The State should fund a study whose goal is to develop a more fine-grained understanding from industry as well as local/federal government precisely which skills are in demand, and how much demand there is for each skill. This would enable tailoring education in cybersecurity accordingly, and would also allow for better matching of students to open positions.

14. Transition Path for Community-College Graduates

Community colleges can also play an important role in increasing the number of cybersecurity professionals. Of particular note is a $5 million grant awarded by the US Department of Labor to Maryland community colleges to support cybersecurity training, certificates, and associate degrees. The State should focus on developing transition paths for community-college graduates in cybersecurity-related fields who wish to transfer to 4-year universities or the workforce.

15. Funding Academic Research

Academic research also plays an important role in cybersecurity education. Besides the benefits that accrue from the research itself, it also serves as an important component of training students at the Masters and PhD levels. These graduates will not only be employed by existing cybersecurity companies, but will also be the ones to form new companies with the next generation of cybersecurity innovations. The State should consider funding academic research in cybersecurity, driven by the cybersecurity needs and challenges of State and local government.

Economic Development

16. Cybersecurity Accelerator

The Council recommends that Maryland establish a statewide cybersecurity accelerator program to help young cyber companies find a firm footing in the marketplace. Cyber accelerator programs offer the training necessary to build and grow a cybersecurity company.

They provide advice, mentoring, and other forms of assistance for businesses in the startup phase, but do so on a compressed timetable. The training could include, for example, advice on team building, business and marketing strategies, and addressing tax and legal concerns. Launching a statewide accelerator, perhaps even one that is a public-private partnership, would expand the number of businesses that could take advantage of the professional support and guidance provided. An accelerator program of this kind should be coupled with incentives to ensure that companies graduating the program remained in Maryland. This would promote economic growth in Maryland's cybersecurity industry.

Public Awareness and Community Outreach

17. Cybersecurity Repository

The Council recommends creating an online repository of cybersecurity outreach, awareness and training information available to private and public sectors as well individuals. For maximum impact, this repository should reside within a State agency that has the capacity to maintain and update the information on a regular basis. The Department of Information Technology appears to be the appropriate agency to host and maintain the repository. The key steps needed to create the repository are as follows:

1. Assess existing cyber security awareness repositories, either federal, state or local levels
2. Conduct research of existing repositories and determine how Maryland can use or leverage those resources
3. Assess, using data from the surveys, what information would be valuable
4. Determine what, if any, new materials need to be developed
5. Determine which State agency would host the repository
6. Create a master list of outreach materials/information, including the targeted audience for the specific information
7. Work with State agency to implement the repository

The online cybersecurity repository and the proposed educational infrastructure have several overlapping goals and, therefore, could be could be a joint project. The Council would work with the selected State agency to implement the repository.

VI. Conclusion

A successful cyber attack against any of Maryland's critical infrastructure will almost certainly have catastrophic consequences to the State's economy, vital services, and the public health and safety of its citizens. The State has a responsibility to secure its critical infrastructure as well as the data that has been entrusted to it by their citizens. In this initial report, the Council has proposed several recommendations to improve the cybersecurity of critical infrastructure entities and advance cyber innovations and jobs in Maryland. The Council looks forward to continuing its work and expanding upon these recommendations in its first full report, due to the Maryland General Assembly on July 1, 2017.