Maryland Cybersecurity Council Activities Report

July 1, 2017

Table of Contents

I. Introduction

This is the first biennial report of the Maryland Cybersecurity Council to the General Assembly.[1] It discusses the status of the recommendations that the council published in its *Initial Activities Report (July 1, 2016)*.[2] This report also looks ahead to the next two years. The council's 2016 recommendations were ambitious. Consequently, some of them will continue to command the council's attention. Moreover, the council's work has focused on new concerns. These are reflected in nine additional recommendations.

To date, the council's impact has principally been in two areas:

Consumer protection. Maryland of course is no stranger to the exposures that our wired society has produced. In a snapshot recently published, the Office of the Maryland Attorney General reports that in Fiscal Year 2016 alone there were 564 data breaches affecting more than 600,000 Maryland residents. The breaches were due to phishing, retail malware, lost or stolen laptops or other devices, unauthorized access, and inadvertent administrative error, such as mistakenly sending personal identifying information to third parties not authorized to have it.[3]

In its 2017 session, the General Assembly enacted bills to expand the protections under Maryland Personal Information Protection Act (SB 525/HB 974) and to waive data breach victims' fees for a credit freeze (SB 270/HB 212). It also held hearings on bills to specifically make ransomware a crime (SB 405/HB 340) and to provide a right of private action for unauthorized computer or network intrusions (SB 287/HB 772). *The snapshot data breach report and versions of these bills all originated in specific recommendations of the council.*

Curation of Resources and the Launch of Best Practices Portal. The exposures to Maryland go beyond data breaches and extend to the State's critical infrastructure (CI).[4] The electrical grid, Maryland's banks, its trains and port facilities, its public and private water treatment and supply plants, hospitals, and more are all targets for cybersecurity attacks and disruption. The ransomware attacks experienced by Maryland hospitals this year bring these risks into focus. Yet these risks extend to all businesses. Particularly vulnerable are small and medium-size enterprises that do not have the deep financial and professional cybersecurity resources of much larger organizations.

To assist smaller CI entities, other businesses, and consumers, the council has begun to curate a collection of resources and best practices and has designed a portal to make them easily accessible. Created with the assistance of the Maryland Department of Information Technology (DoIT), the portal will be available as a link on websites of the Office of the Attorney and the Maryland Cybersecurity Council. The portal will be available in the fall of 2017.

[1] The report is required by SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 Section 3.

[2] The report may be found at http://www.umuc.edu/mdcybersecuritycouncil

[3] See http://www.marylandattorneygeneral.gov/Reports/FY2016_Data_Breach_Snapshot_Report.pdf and http://www.umuc.edu/mdcybersecuritycouncil

[4] For critical infrastructure sectors, see https://www.dhs.gov/critical-infrastructure-sectors

As part of this report, it is important to note that one of the council's statutory charges has been accomplished by other state agencies. The law directs the council "to recommend a comprehensive plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks".[5] At the time the council was created, the state had already begun this effort. The *State of Maryland Cyber Disruption Plan* was finalized after a cross-agency exercise in 2016 and was signed by the executive director of the Maryland Emergency Management Agency (MEMA) and the acting secretary of DoIT in 2017.

While the completion of the *Cyber Disruption Plan* is a significant milestone, one of the council's new concerns is the rate at which the state government is investing in its core cybersecurity capabilities. State governments and their agencies hold volumes of personal data and business information, provide services, and play a critical role in responding to emergencies.[6] State chief security officers identify insufficient funding, inability to recruit cybersecurity professionals, lack of visibility within the enterprise, and the increasing threat sophistication as among their top challenges in addressing network security risks.[7] A recent report notes that the federal, state and local governments in the United States are ranked at the bottom when compared with 17 major industries across a variety of cybersecurity metrics.[8] One of the council's own subcommittees raises significant concerns about Maryland's cybersecurity posture and the level of security funding.[9] While there is an awareness among Maryland officials of the threats facing the state, the question is whether capacity-building should be accelerated. A similar question about the priority of cybersecurity investments can be raised about Maryland local governments.

---

[5] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 Section 9-2901(J)(6).

[6] For an assessment of cyber threats against state and local government in 2017, see *2017 SLTT Government Outlook*. White Paper. Center for Internet Security (January 2017) at https://www.cisecurity.org/wp-content/uploads/2017/03/SLTT-Outlook-2017.pdf. There are a variety of more general threat trend reports. For example, see Symantec, *Internet Security Threat Report*. Vol 22 (April 2017) at https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-APR24.pdf?aid=elq_; CrowdStrike, *Cyber Intrusion Services Casebook 2016* at https://www.crowdstrike.com/resources/crowdcasts/cyber-intrusion-services-casebook-2016/; and Mandiant/FireEye, *M-Trends 2017, at* https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

[7] The 2016 Deloitte-NASCIO Cybersecurity Study, *State Governments at Risk: Turning Strategy and Awareness into Progress*, p.7, at https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress. See also Ponemon Institute, *State of Cybersecurity in Local, State and Federal Government*. (October 2015), p. 8, at http://www.ponemon.org/blog/the-state-of-cybersecurity-in-local-state-and-federal-government.

[8] *2016 US Government Cybersecurity Report*. SecurityScoreCard (April 2016), p. 6. This report is available at http://info.securityscorecard.com/2016-us-government-cybersecurity-report and is cited in *Cyber Threats Facing State and Local Government.* Accenture (2016) at https://www.accenture.com/t20160913T145717__w__/us-en/_acnmedia/PDF-30/Accenture-Cyber-Threats-Facing-State-Local-Government.pdf

[9] See the report of the council's Cyber Operations and incident Response Subcommittee in Appendix C. See also a third-party assessment of Maryland's security posture that places the state "in the bottom ten state organizations with the weakest security posture", *2016 US Government Report*. SecurityScoreCard, p. 9.

II. Council Overview

Council Mission

The council's statutory charge is to assess the cybersecurity risk of critical infrastructure in Maryland, to assist critical infrastructure entities not covered by Federal Executive Order 13636 to meet federal cybersecurity guidance, to encourage and assist private sector firms to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to identify regulatory inconsistencies between State and Federal cybersecurity law that may complicate compliance by Maryland businesses, to support the creation of a cybersecurity resiliency plan for the State, and to recommend any other legislation to address cybersecurity issues.[10]

Council Organization & Membership

By statute, the council is chaired by the Attorney General or the Attorney General's designee.[11] It currently consists of 50 other members organized into six subcommittees. The council's composition reflects a 'whole of community' approach to addressing cybersecurity issues.[12] The membership is a mix of statutorily designated and discretionary seats with appointments reserved either to the Attorney General, the President of the Senate, or the Speaker of the House, depending on the case. Represented are key federal and state departments, state legislators, and various sectors of Maryland civil society: critical infrastructure entities, higher education, small businesses, statewide business and technology associations, and crime victim's groups, among others.[13] In addition to its appointed members, the council has attracted a number of "contributors" to its work, viz. private citizens who are not appointed members but who are willing to give council initiatives their time and expertise.

The subcommittees, their objectives and current appointed members are as follows:

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
- Ned Carey, Delegate, Maryland General Assembly
- Howard Feldman, Esq., Attorney, Whiteford, Taylor & Preston

[10] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 (J)
[11] Ibid, §9-2901 (G)
[12] Ibid, §9-2901(C)-(F)
[13] For members grouped by sector, see Appendix A.

- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland, Baltimore
- Joseph Morales, Esq., Attorney, Maryland Hispanic Chamber of Commerce
- Jonathan Prutow, Policy and Planning Business Analyst, Macro Solutions
- Paul Tiao, Esq., Attorney, Hunton & Williams
- Pegeen Townsend, Vice President, Government Affairs, Medstar Health

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

Subcommittee Members

- Chair: Michael Leahy, Acting Secretary of DoIT
- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System
- Robert W. Day Sr., Senior Security Monitoring Analyst, AECOM, Inc.
- Judith Emmel, Associate Director, State, Local, and Community Relations, National Security Agency; liaison to the council
- Mary Ann Lisanti, Delegate, Maryland General Assembly
- Anthony Lisuzzo, Board Member, Army Alliance
- Walter "Pete" Landon, Director, Governor's Office of Homeland Security
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Colonel William Pallozzi, Maryland Secretary of State Police

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, John M Francis King Carey School of Law, University of Maryland, Baltimore
- John Abeles, President and CEO, System 1, Inc.
- Dr. David Anyiwo, Chair, Department of Management Information Systems, Bowie State University
- Mark Augenblick, Esq., 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.
- Bryan Simonaire, Senator, Maryland General Assembly
- Major General 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 for developing programs for students and professionals entering the cybersecurity field
    - Recommendations for attracting teachers and faculty qualified to teach cybersecurity courses in high school and beyond
    - Recommendations for developing and modifying high school and higher education curricula 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 for 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
- Shiva Azadegan, PhD, Director, Computer Science, Towson University
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove, University System of Maryland
- Henry J. Muller, Director, Communications-Electronics Research, Development and Engineering Center, U.S. Army, Aberdeen Proving Ground
- Jonathan Powell, Senior Director, Software Engineering, GDIT
- 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, such as attracting venture capital and offering 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
- James Foster, CEO, ZeroFox
- Don Fry, President and CEO, Greater Baltimore Committee
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Tami Howie, CEO, Tech Council of Maryland
- Brian Israel, Business Development Executive, MACPA
- Ronald Kaese, Director, Federal Programs, Maryland Technology Development Corporation (TEDCO)
- Ken McCreedy, Senior Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- Steven Tiller, President, Fort Meade Alliance

Public Awareness and Community Outreach Subcommittee

Subcommittee Objectives

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

Council Staffing

The University of Maryland University College (UMUC) is the staffing agency for the Maryland Cybersecurity council.[14] The university has been designated as a National Center of Academic Excellence in Information Assurance and Cyber Defense Education by the National Security Agency and the Department of Homeland Security and as a National Center of Digital Forensics Academic Excellence by the Defense Cyber Crime Center Academic Cyber Curriculum Alliance.

III. The Council's 2016 Recommendations

The council has met six times since its inception in July 2015.[15] The goals of the initial year (July 2015 – July 2016) were to appoint council members, to create subcommittees and to formulate a roadmap of initiatives on which the council would begin work. The result was 17 recommendations published in the council's *Initial Activities Report*.

2016 Recommendations		Originating Subcommittee
1.	Creation of Cyber First Responder Reserve	Law, Policy, Legislation
2.	Updates to the Maryland Personal Information Protection Act	
3.	Civil Cause of Action for Remote Unauthorized Intrusions	
4.	Facilitating Use of the No-charge Credit Freeze Option	
5.	Inclusion of NIST Cybersecurity Framework in the State IT Master Plan	
6.	Publication of a Maryland Data Breach Report	
7.	Integrated Cyber Approach for Mid-Atlantic Region	Cyber Operations & Incident Response
8.	Educational Resources for Critical Infrastructure Owners and Operators	Critical Infrastructure
9.	Identify Maryland Critical Infrastructure and Risk Assessments	
10.	Basic Computer Science and Cybersecurity Education	Education & Workforce Development
11.	Maryland Cybersecurity Scholarship for Service	
12.	Resources for University Computer Science Departments	
13.	Study of Cyber Workforce Demand and Skills	
14.	Transition Path for Community College Graduates	
15.	Increased Funding for Academic Research	
16.	Cybersecurity Business Accelerators	Economic Development
17.	Cybersecurity Repository	Public Awareness & Outreach

[14] Md. Ann. Code, St. Gov't Art. §9-2901 (H)

[15] See http://www.umuc.edu/mdcybersecuritycouncil

As part of its due diligence both to prepare its recommendations and to begin realizing them, the council arranged expert presentations at its meetings. These included briefings by Charles Ames, DoIT director of cybersecurity, and Colonel Shawn Bratton, commander of the 175th Wing Cyberspace Operations Group, Maryland Air National Guard. Likewise, the council organized receptions in Annapolis in both 2016 and 2017 for legislators and their staff on the internet and security-related issues. These respectively featured:

Vinton Cerf, vice president and chief internet evangelist at Google. Dr. Cerf noted that the cybersecurity risks are mounting and that the efforts to address those risks have not been adequate. He emphasized that cybersecurity is both a public and private responsibility. Government should model cybersecurity best practices. Similarly, through a combination of market incentives and regulation, infrastructure providers, software developers, and device manufacturers should be spurred to build in more security. He commented on the particular vulnerability of small businesses and suggested a "cyber fire department" that would be available to assist them when their networks are compromised. He underscored the great possibilities offered by the Internet of Things (IoT), but also the increased opportunity for harm and the enlarged risks to privacy.

Dmitri Alperovitch, co-founder and CTO at CrowdStrike. Based on CrowdStrike's 2016 cyber casework, Mr. Alperovitch discussed the attack trends that he anticipated in 2017. He also explored the improvements that have been made in the ability to identify the source of cyber attacks, providing examples involving Russia and China. His presentation captured a list of take-aways for governments and businesses to better secure themselves. These included better credential management, social engineering awareness training, attention to supply chain security, and a number of other policy and technology recommendations.

Combining its own interests with its public outreach mission, the council organized a Public Policy Forum on December 6, 2016, for citizens, private industry representatives, and policymakers. The event was held at University of Maryland University College and focused on privacy issues and critical infrastructure risk. Chaired by Attorney General Brian Frosh, the symposium included two sessions respectively led by Maryland Senator Susan Lee and Professor Michael Greenberger, director of the Center for Health and Homeland Security at the University of Maryland Francis King Carey School of Law. Panelists included Dr. Phyllis Schneck, then-deputy under secretary for cybersecurity and communications for the National Protection and Programs Directorate (NPPD), US Department of Homeland Security (DHS); Allison Lefrak, senior attorney for privacy and IP protection, Federal Trade Commission; and Claire Gartland, director of the Consumer Privacy Project, Electronic Privacy Information Center.

IV. Status of the 2016 Recommendations

In the 12 months since they were published, several of the council's recommendations have been implemented because of the support of key policymakers and stakeholders. The council's initial impact has been in the areas of consumer protection and the creation of soon-to-be publicly available, curated resources for CI entities, small and medium businesses, and consumers. However, even where the council's subcommittees have not been able to convert recommendations into initiatives, they are continuing their efforts to do so.

Law, Policy and Legislation Subcommittee

Recommendation 1. Cybersecurity First Responder Reserve
Status: Work Ongoing
The subcommittee continues to accumulate information to shape the concept of a reserve and to inform the legislative proposal that may be necessary to implement it. This information includes the activity of the Maryland National Guard's cyber operations units and the role of the Maryland Defense Force[16] that is under the command of the governor and the operational control of the adjutant general. It also has included discussions with MEMA.

MEMA has noted that its role in relation to a cyber first responder group would be the same as it is now with respect to other groups involved in an emergency response. Specifically, MEMA would be the coordinating agency with DoIT as the lead agency. DoIT has completed a full incident response plan with MEMA participating in that effort. When a first responder group would be activated, it would have to be integrated into that plan.

Other points pertinent to establishing a cyber first responders reserve include the following:

- If the emergency involved private critical infrastructure, there would need to be coordination with the private sector, since the state does not have direct control of private entities.
- The state does not have a list of specific public and private infrastructure entities falling within the 16 DHS critical infrastructure categories.
- If a first responder reserve is authorized and formed, MEMA will need additional funding to manage or coordinate it. Now, 75 percent of MEMA's funding is from the federal government.
- MEMA and DoIT have exercised a cyber emergency (table top), but more exercises will follow to identify gaps in communication, coordination, equipment, and technical talent to refine the plan and better prepare for its execution.

Recommendation 2. Updates to the Maryland Personal Information Protection Act
Products: SB 525/HR 974 passed in the 2017 session accomplishing key changes recommended by the council
Status: Work Ongoing
Maryland's Personal Information Protection Act was first passed in 2008 and was among the first in the nation. The statute defined "personal information" to include first name or first initial and last name in combination with social security number, driver's license number, tax identification number, and credit or debit card account numbers that in conjunction with a security code or password would permit access to financial information. Further, the statute's definition of a breach included the acquisition of data but did not include "access" where data could be altered. Finally, the statute's required notification to Maryland consumers and the attorney general's office was formulated as a standard, "as soon as reasonably practicable".

As proposed by the subcommittee, the General Assembly in the 2017 session was responsive to broadening the definition of personal identifying information to include health information (including mental health information), health insurance policy or certification subscriber

[16] See http://mddf.maryland.gov/index.aspx and http://mddf.maryland.gov/blogpost.aspx?id=17.

identification numbers, certain biometric data, the passport number and other identification numbers issued by the federal government or the State of Maryland, and usernames and email addresses that in combination with a password would permit access to an email account.[17] In addition, the General Assembly defined the breach notification requirement to be no longer than 45 days in most cases, a change that benefitted businesses as well as consumers by removing uncertainty about the "reasonably practicable" standard.[18] The revised statute avoided increasing regulatory burdens by providing safe harbor for firms already subject to federal regulation under the Health Insurance Portability and Accountability Act (HIPPA).[19] Safe harbor already existed in the 2008 statute for firms covered by the Gramm-Leach-Bliley Act and those encrypting personal identifying data that they hold.

While the council's recommendation was advanced in significant ways, the subcommittee will continue its effort to realize "unauthorized access" *per se* as the notification trigger in the statute and to accomplish other changes that the council endorses. These include providing protection for non-HIPPA entities holding health information, protecting the credit card information of small businesses, and clarifying the "state-wide" notification requirement.

Recommendation 3. Civil Cause of Action for Remote Unauthorized Intrusions
Products: SB 287/HB 772 was proposed but did not pass in the 2017 session.
Status: Work Ongoing
Acting on the council's recommendation, the subcommittee submitted a bill in the 2017 session to provide this remedy. It aimed a) to make it an offense to undertake certain actions that could compromise the confidentiality or integrity of data stored on a computer or network or cause damage to those systems; b) defined a range of penalties for these actions, including fines and imprisonment; and c) provided for the right of civil action for victims of offenses under the bill. The bill was withdrawn to permit the subcommittee more time to address several questions that legislators raised.

Recommendation 4. Facilitating Use of No Charge Credit Freeze Option
Products: SB 270/HB 212 was proposed in the 2017 session and become law without the governor's signature. (Enacted under Article II, Section 17(c) of the Maryland Constitution) - Chapter 828.)
Status: Closed
The credit report freeze is a mitigation tool that consumers can use to reduce the impact of identity theft. The freeze restricts access to credit reports, making it difficult for identity thieves to open new accounts in someone else's name. Currently, a $5 credit report freeze fee for each of the three credit reporting agencies is waived when identity theft has already occurred. The council recommended removing the fees associated with initiating a credit freeze as soon as a data breach is reported to encourage proactive consumer protection. As enrolled, SB 270/HB 212 waives data breach victims' fees for a credit freeze, incentivizing individuals to obtain a freeze before new accounts are fraudulently created.[20]

[17] HB 974, amending Md. Ann. Code, Comm. Law Art. §14-3501 (e).
[18] HB 974, amending Md. Ann. Code, Comm. Law Art., § 14-3504 (b)(3), (c)(2) and (d)(2).
[19] HB 974, amending Md. Ann. Code, Comm. Law Art. §14-3507 (c) and (d)
[20] HB 212, amending Md. Ann. Code, Comm. Law Art. §14-1212.1 (i)(3)

Recommendation 5: Inclusion of the NIST Cybersecurity Framework in the State IT Master Plan
Products: SB 286 was proposed but no legislative action taken in the 2017 session.
Status: Work Ongoing
The *Cybersecurity Framework* was developed by NIST as a voluntary framework with wide input from industry, government and academic experts.[21] While it was originally intended for the critical infrastructure sectors, the *Framework* is finding wide adoption across the United States. Most recently, the new Executive Order of the president directs federal Executive Branch agencies to implement the Framework and any successor document to manage their cybersecurity risk.[22] In addition to the *Framework*, there are several cybersecurity standards—such as ISO to which it is mapped. The bill did not move beyond the hearing committee. Similar bills were proposed in the three prior legislative sessions with the Senate passing them in 2014 and 2015. DoIT has committed to meeting the objectives of the *Framework.*

Recommendation 6: Publication of a Maryland Data Breach Report
Products: FY 2016 Data Breach Snapshot Report
Status: Closed
While there are numerous reports about data breaches and identify theft, the council had recommended that the Office of the Attorney General publish a data breach report focused specifically on Maryland. This data is available because of the notification requirements of the Maryland Personal Information Protection Act and a similar statute pertaining to state agencies. The council's goal is to aid policymaking by providing citizens and officials with more information about the exposure of Maryland consumers to this cybersecurity risk. The Office of Attorney General welcomed the recommendation and published its initial report in June.[23] This report will be updated annually.

Cyber Operations and Incident Response Subcommittee

As noted earlier, the council's enabling statute directed it to create "a comprehensive state strategic plan to ensure a coordinated and adaptable response to and recovery from cybersecurity attacks.[24] Because the council understood that DoIT had already begun that effort, the creation of the plan was not included as a numbered recommendation of this subcommittee in the *Initial Activities Report.* The council resolved to support the efforts of DoIT as the lead agency.

DoIT completed the *State of Maryland Cyber Disruption Contingency Plan* earlier this year. As a complement to the state's *Consequence Management Operations Plan CMOP),* it describes the strategy to coordinate state-level operations to support local, state, and federal agencies in addressing potential or actual disruptions from a cyber-attack. The plan was first exercised cross-agency in April 2017.

Recommendation 7. Integrated Cyber Approach for the Mid-Atlantic Region
Status: Work Ongoing

---

[21] See https://www.nist.gov/cyberframework/draft-version-11
[22] Executive Order of the President, Strengthening the Cybersecurity of the Federal Networks and Critical Infrastructure, Section 1 (c)(ii)(B) and (iv)(B)(5) at https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
[23] See http://www.marylandattorneygeneral.gov/reports/FY2016_Data_Breach_Snapshot_Report.pdf
[24] Md. Ann. Code, St. Gov't Art. §9-2901 (j)(6).

Based on its research, the subcommittee concluded that the state should have in place a number of building blocks before it can effectively participate in a multi-state cyber incident response regime. While not losing sight of this recommendation, these building-block initiatives are identified as new council recommendations in Section V.

Critical Infrastructure and Cybersecurity Framework Subcommittee

Recommendation 8. Educational Resources for Critical Infrastructure Owners and Operators
Products: Resources curated for Cyber Resources and Best Practices Portal
Status: Work Ongoing.

In the *Initial Activities Report*, the subcommittee recommended the establishment of an educational infrastructure to inform and support critical infrastructure owners and operators, as well as other stakeholders, on cybersecurity matters. This infrastructure will provide resources to Maryland critical infrastructure sectors and other stakeholders in the state. These information resources are based on the latest cybersecurity trends, guidance, and best practices.

Based on this and other subcommittees' recommendations, the council proposed that the state establish a public portal that will provide cybersecurity resources and educational materials to critical infrastructure owners and operators and other stakeholders.

The subcommittee recommends that the portal include information on the following topics:

- General cybersecurity awareness
- Information sharing through information sharing and analysis organizations (ISAOs)
- Cybersecurity frameworks, including the NIST *Framework*
- Critical infrastructure tools for cybersecurity
- Cyber risk management
- Cyber workforce development and training
- Other subjects based on stakeholder demand

The subcommittee has collected specific resources to address these topics.[25] During the next two years, the subcommittee will continue to pursue Recommendation 8 to ensure that resources remain current.

Recommendation 9. Identify Maryland Critical Infrastructure and Risk Assessments
Products: Resources curated for Cyber Resources & Best Practices Portal.
Status: Work Ongoing
Risk Assessment
Risk assessments are one of the best ways for organizations to determine vulnerabilities and their potential consequences. In the *Initial Activities Report*, the subcommittee recommended that the state gather tools and outline steps to help critical infrastructure owners and operators to conduct risk assessments with respect to cyber incidents. The state should furthermore encourage the performance of risk assessments in order to make these sectors more resilient.

As previously highlighted, the recommended set of tools and "best practices" for infrastructure protection must include the use by critical infrastructure sectors of the NIST *Framework* which is

[25] See Appendix B

currently being updated. Use of the *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 C³ Voluntary Program, which supports stakeholders in their use of the NIST Framework. Furthermore, the subcommittee recognizes that some suppliers of critical infrastructure may be compelled to adhere to alternative frameworks developed by the International Organization for Standardization (ISO) or the Health Information Trust Alliance (HITRUST), for example.

DHS 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 (NPPD) 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[26]
- Self-evaluation tools, such as those made available through the United States Computer Emergency Readiness Team (US-CERT)
- 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
- Training opportunities that include courses on critical infrastructure protection and security

The subcommittee has collected additional resources to support critical infrastructure in conducting risk assessments and will continue to update them.[27]

Identification of Critical Infrastructure Sectors at Greatest Risk and Their Interdependencies

The subcommittee has worked on determining which local critical infrastructure sectors are at the greatest risk of cyber attacks and therefore need the most enhanced cybersecurity measures. The subcommittee 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

[26] 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.

[27] Appendix B

These sectors are critically important to Maryland as well. It is also important to note that each of these sectors is vulnerable and that the threat environment is fluid. Much of the information on sector-specific vulnerabilities is sensitive and not available for a public report. The conclusions that the subcommittee may make within this report are therefore limited.
In addition to analyzing vulnerabilities of specific critical infrastructure sectors, the subcommittee focused much of its efforts on highlighting the interdependencies between critical infrastructure sectors. The state is dependent on critical infrastructure systems to provide essential services that support economic prosperity, governance, and quality of life. These systems are not independent, but rather interdependent at multiple levels to enhance their overall performance. An attack on one critical infrastructure sector will likely have a decisive negative effect on the functioning of other infrastructures. For example, a cyber attack that successfully disables a power plant or electric grid will have the effect of shutting down other sectors that rely on electricity. The interdependence between infrastructures requires those involved in defending from such attacks to adjust to this reality and prepare accordingly.

Moreover, the subcommittee reiterates that interdependencies exist not only between sectors, but also geographically. While the council's enabling statute references "local" infrastructure sectors[28], this subcommittee recommends that state planners and critical infrastructure owners and operators examine interdependencies 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.

In order to ensure that interdependencies between sectors are considered in all planning efforts, the subcommittee has collected resources to support state planners and critical infrastructure owners and operators. Critical infrastructure must focus on the potential for cascading vulnerabilities that depend on the level of interdependency between sectors. There is a necessity to adopt a holistic, multi-disciplinary approach to the vulnerability analysis of critical infrastructures systems.

Relevant resources and materials pertaining to the challenge of addressing critical infrastructure interdependencies have been compiled by the subcommittee.[29] The resources made available to critical infrastructure must be based on the latest cybersecurity trends, guidance, and best practices. As such, the subcommittee will continue its work to ensure that these resources are kept relevant and up-to-date. The subcommittee will continue to rely on its members to provide useful and practical guidance to critical infrastructure owners and operators in Maryland.

Education and Workforce Development Subcommittee

Of the six recommendations that the council endorsed, the subcommittee focused on three.

Recommendation 10. Basic Computer Science and Cybersecurity Education
Status: Work Ongoing
Several efforts to improve computer-science (CS) education at the K-12 level are already underway, both in the State of Maryland as well as nationwide. In particular, the Maryland State

[28] Md. Ann. Code, State Gov't Art. §9-2901(j)(1)
[29] Appendix B

Department of Education (MSDE) has made progress in this area over the past year. In collaboration with stakeholders from across the country, they have developed a preK-12 CS framework that defines what all students should know about CS concepts and skills.[30] Maryland's own CS framework was released about one year ago. MSDE has also developed a toolkit containing free instructional resources to support implementation of Maryland's CS framework.[31] In addition, MSDE has implemented policies that would allow CS courses to fulfill graduation credits for technology and/or mathematics.

The subcommittee also notes that there is at least one state-level workgroup looking at K-12 CS education for the State of Maryland as part of the Governor's Task Force on Workforce Development. The subcommittee will seek to engage that workgroup to understand its initiatives.

The subcommittee identified several challenges to focus on in the 2017 - 2019 period:

- It is extremely difficult to find qualified CS teachers at the K-12 level. Most of the existing math, science, and technology teachers do not have expertise in computer science; college graduates with expertise in computer science encounter a very strong hiring market in industry and tend not to go into teaching at the K-12 level. It seems imperative to develop programs that can help provide training in CS for existing teachers as well as college graduates in related fields who are interested in becoming teachers.

- The CS curricula that have been developed so far do not place sufficient emphasis on cybersecurity. There remains a need to integrate basic cybersecurity principles and awareness in the CS content at the K - 12 level.

Recommendation 11. Maryland Cybersecurity Scholarship for Service
Status: Work Ongoing
The US Scholarship for Service program provides students with funding for up to two years of their degree in return for which recipients must commit to working for the US government for an equivalent number of years after graduation. The State of Maryland should consider implementing a similar program focused specifically on cybersecurity. This would require identifying suitable positions that the state needs to fill and understanding how such positions are currently filled.

The subcommittee observed that this idea could help address the challenges identified above if students could fulfill their service to the State of Maryland by teaching CS at the K - 12 level. More generally, the State of Maryland could consider funding scholarships specifically for students who want to go into teaching CS at the K - 12 level.

Recommendation 13. Study of Cyber Workforce Demand & Skills
Status: Closed
In initially formulating this recommendation, the council was concerned about the need for a common vocabulary to talk about cybersecurity roles, for a database of granular information about the cybersecurity skills employers are seeking, and for a mapping of those skills to

[30] See http://k12cs.org
[31] See http://msdecomputerscience.weebly.com

available training and education opportunities. The subcommittee believes that these concerns are now being substantially met by NIST and its National Initiative for Cybersecurity Education (NICE).

First, the NICE Initiative has produced a *National Cybersecurity Workforce Framework*[32] *(NCWF).* The NCWF groups cybersecurity work into seven categories and breaks each down into specialty areas, work roles, tasks and KSAs. The NCWF is based on extensive job analysis and is independent of job titles which vary from organization to organization. The NCWF has been integrated into the US Department of Labor's Cybersecurity Competency Model and provides a common language for talking about cybersecurity.[33]

Second, in November 2016, NIST announced a tool called *Cyberseek* that offers a granular view of cybersecurity workforce needs.[34] The tool was developed under a grant from NIST, involves a partnership between CompTIA and Burning Glass Technologies, and is refreshed periodically. It is based on the NCWF and includes a "Career Pathway" that helps students, career counselors, and cybersecurity job seekers to understand the requirements of cyber jobs and cyber career progressions as they exist in the market.

In addition to the ongoing efforts identified above, the subcommittee will consider appropriate ways to advance:

- Recommendation 12. Resources for University Computer Science Departments
- Recommendation 14. Transition Path for Community College Graduates
- Recommendation 15. Increased Funding for Academic Research

Economic Development Subcommittee

Recommendation 16. Cybersecurity Business Accelerators
Product: HB 873 (Income Tax Credit – Security Clearances – Employer Costs Extension) passed in the 2017 session
Status: Work on Recommendation 16 is Ongoing as a Multifaceted Initiative
The subcommittee is charged with developing initiatives to support entrepreneurship in cybersecurity, to recruit established cybersecurity firms to Maryland, and to create a business environment that will help cybersecurity firms grow and remain in the state. The subcommittee focused on two strategies relating to its charge:

- To develop an asset map tool for cyber businesses. The subcommittee used the business life cycle as the framework for thinking about the specific needs of cybersecurity business at each stage of their development and for identifying the assets available for these firms. The lifecycle stages are:

[32] See https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework. A draft revision of the NCWF can be found at http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf
[33] See http://www.careeronestop.org/CompetencyModel/competency-models/cybersecurity.aspx
[34] See https://www.nist.gov/news-events/news/2016/11/nist-announces-cyberseek-interactive-resource-cybersecurity-career and http://cyberseek.org/

    - Stage 1: Startup (seed and development)
    - Stage 2: Growth
    - Stage 3: Maturity
    - Stage 4: Expansion
    - Stage 5: Decline and Possible Exit
- To formulate incentives and investment ideas that might be translated into legislation.

Asset Map Tool

While under active discussion within the subcommittee, this project was adopted by the Maryland Department of Commerce which had independently been considering a similar idea. Its asset map will identify resources across Maryland that could be leveraged by cybersecurity firms at any point in their lifecycle, from start-up to maturity. This effort will identify cybersecurity companies in the state; list their primary product and/or service; locate them; indicate whether their primary customer is government, commercial, or both; and collect other pertinent facts. In addition, the map will show workforce pipeline sources such as college and university cybersecurity degrees and programs, K - 12 educational initiatives aimed at cybersecurity skills and literacy, training programs, and apprenticeship programs. The map will also show innovation hubs where cybersecurity start-ups are located and special programs available to assist cybersecurity companies. The Cyber Asset Map will be unveiled as part of CyberMaryland in October 2017. At the subcommittee's recommendation, the council has proposed that the asset map be linked to the business lifecycle to enhance its usefulness.

Incentives and Investment ideas

The council's Economic Development Subcommittee is only one of a number of public entities looking at ways to accelerate business growth in the state. The governor's Workforce Investment Board, his Excel Maryland initiative, and the Maryland Department of Commerce, among others, are of course focused on this question. The subcommittee's efforts relating to cybersecurity business sector included the following:

- HB 873 was sponsored by Delegate Ned Carey, the legislative member of the subcommittee. The bill extends through tax year 2021 the tax credit allowed against the Maryland income tax for certain costs related to establishment of secure compartmented information facilities (SCIFs) in the state. HB 873 continues to permit the state to award $2 million in total credits each year for the period of the extension.[35]

- The subcommittee examined whether state procurement practices intended to support Maryland firms are in line with those of many other states. The subcommittee confirmed that Maryland law provides that resident firms should be awarded the same preferential advantage in state procurements against out-of-state firms that those firms enjoy in their home state against Maryland firms.

- Aware of the role that blockchain and artificial intelligence will play in cybersecurity, the subcommittee also raised the question whether the statute establishing the Technology Development Corporation (TEDCO) should be amended to make investment funds available

[35] HB 873, amending Md. Ann. Code, Tax Article, §10-732 (b)

for commercialization of these tools. Once again, the subcommittee confirmed that TEDCO does not need additional authority to invest in these areas.

In the next two years, the subcommittee will consider additional proposals to support the development and growth of the cyber-related business sector in Maryland in concert with other initiatives. These include but are not limited to:

- A substitute package for the Investment Tax Credit
- Income tax and other incentives to give Maryland an edge in recruiting skilled professionals into the state; and
- Incentives for firms to take on student interns to accelerate their security clearance process

Public Awareness and Community Outreach Subcommittee

Recommendation 17. Cybersecurity Repository
Products: Mock-up of website portal completed, initial resources identified, host identified.
Status: Work Ongoing
The council recommended that the state launch a repository of curated resources that would be helpful to consumers, small infrastructure owners, and other businesses. While many resources area available, knowing where to look and sifting them for usability is a challenge. In response to this recommendation, the subcommittee made considerable progress:

Content. It partnered with the subcommittee on Critical Infrastructure to develop an initial set of curated resources that includes use cases to highlight the relevance of the resources.
Portal. The subcommittee worked through the last year with DoIT to develop and host the website landing page for the resources.
Audience. To connect consumers and small businesses with the repository, the subcommittee has developed a list of organizations it recommends to highlight the repository on their websites.

The subcommittee will finalize the website design in consultation with the Office of the Attorney General and create a protocol for managing the site so that the resources remain current and grow. The website will be launched in the fall 2017.

In the 2017-2019 period, the subcommittee will remain active in expanding the content of the repository so that it can become a robust resource for CI entities, small and medium businesses and consumers.

V. New Council Recommendations for 2017 – 2019

The six subcommittees will continue their efforts to fully realize the recommendations already identified in the *Initial Activities Report.* Moreover, they have made nine additional recommendations which the council endorses. These are the result of the subcommittees' ongoing research, advancing technology, and persistent threats to Maryland's citizens, critical infrastructure, and state operations.

Law, Policy and Legislation

2017 Recommendation 1. The council recommends legislation that would update the state's Executive Branch breach law and extend personal information privacy protections and breach reporting requirements to the judicial and legislative branches.
This recommendation reflects the belief that the state's Executive Branch breach law should align with the commercial breach law and that similar protections and requirements should apply uniformly across the branches of state government.

2017 Recommendation 2. The council recommends legislation or policy changes that would require state IT procurements to resource and include an independent security verification of device or code readiness and/or system security readiness prior to government acceptance. The *council is sensitive to the recommendation's potential impact on Maryland's business sector and on the cost of goods and services to the state. The council intends that these considerations weigh into a discussion of a regime that would contribute to the cybersecurity of the state.*

The supply chain on which organizations rely is a key area of cybersecurity risk to data and the ability to provide services. This vulnerability is identified in the NIST Framework.[36] As one indicator of risk, only 57 percent of state CIO's in the last NASCIO survey were "somewhat confident" that they can protect their information assets from threats originating from third-parties and only 37 percent were "somewhat confident" that they could control risk from threats emerging from the state's use of emerging technologies, like the Internet of Things.[37]

2017 Recommendation 3. The council recommends legislation that will require express consumer consent for internet service providers(ISPs) to sell or transfer consumer internet browser history.
This recommendation takes notice of Congressional repeal of the Federal Communication Commission regulation prohibiting such sale.[38] Minnesota has already barred ISPs from selling browsing history without the consumer's consent.[39]

2017 Recommendation 4. The council recommends the inclusion of a ransomware definition in the Maryland's extortion statute or a new code section with increased penalties for extortion levels below the general extortion statute threshold.
SB 405/HB 340 was proposed in the 2017 session, and hearings were held on the bill in both the Senate and the House. Given the wide and disruptive use of ransomware, the council continues to recommend that it be specifically named as a crime and penalized in a way not provided for in the current state extortion law.

---

[36] See for example NIST Cybsesecurity Framework ID. AM-6, ID.BE-1, ID. BE-4 and PR.AT-3 at https://www.nist.gov/cyberframework/draft-version-11

[37] *State Governments at Risk: Turning Strategy and Awareness into Progress*. The 2016 Deloitte-NASCIO Cybersecurity Study, p.18, at https://www.nascio.org/Publications/ArtMID/485/ArticleID/413/2016-Deloitte-NASCIO-Cybersecurity-Study-State-Governments-at-Risk-Turning-Strategy-and-Awareness-into-Progress

[38] Senate Joint Resolution 34 pursuant to the Congressional Review Act ("CRA"), 5 U.S.C. § 801.

[39] See the analysis of the National Council of State Legislatures at http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#ISPs

2017 Recommendation 5. The council recommends the right of civil action against former employees in the event of a breach due to intentional conduct that was the proximate cause of actual damages or mitigation costs, with punitive damages available when plaintiff can prove malice.
Many data breaches are caused by those with insider knowledge, including both current and former employees.[40] The recommended legislation would reinforce the continuity of an employee's responsibility to protect sensitive data even after a change employment.

2017 Recommendation 6. The council recommends legislation that would require IoT devices to include consumer labelling about the security features the devices incorporate.
This recommendation reflects the concern about the proliferation of insecure devices that pose undisclosed privacy and safety risks to consumers and can impose massive social costs in the form of devastating Distributed Denial of Service (DDoS) attacks.

2017. Recommendation 7. The council recommends legislation to ensure the transparency to consumers of data held by data brokers about them, the right of consumers to inspect and correct wrong data, and the right to opt out of the sale of their data by brokers for marketing or people search purposes.
The council notes the wide use of data broker products and the lack of transparency or visibility to consumers about who has their data and how it is used and sold.[41]

Cyber Operations and Incident Response Subcommittee & Critical Infrastructure and Cybersecurity Framework Subcommittee

2017 Joint Recommendation 8. The council recommends that Maryland develop capability for sharing cybersecurity information and providing outreach support.
Thwarting cyber-attacks requires rapid sharing of information, from dozens of sources across any size network as well as across traditional critical Infrastructure silos (e.g., transportation, aviation, finance). Sorting through the thousands of threat signatures for the relevant threats to our networks, businesses, and citizens is a challenging and expensive task in terms of labor and equipment costs. After patching, automated information sharing and threat analytics development are foundational to an active defense.

Consequently, both subcommittees recommended that the state establish and expand the ability for stakeholders to accept and share threat intelligence, indicators of compromise, and any other such information that may pertain to the cybersecurity of the state's critical infrastructure. This capability should include:

- Participation in cybersecurity information sharing for state-owned or operated critical infrastructure and for critical infrastructure for which the state directly contracts
- The provision of voluntary participation by all critical infrastructure parties

[40] See https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/employees-commit-most-data-breaches.aspx.
[41] See Data Brokers: A Call for Accountability and Transparency, Section VIII (FTC, May 2014) at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

- Reasonable processes and practices to preserve the confidentiality and rights of submitters of information to this function
- Identification and analysis of any necessary legal implications related to running this function
- The implementation of a plan to operate and sustain this function including, but not limited to:
    - Information sharing/coordination during a cybersecurity event response with events defined as abnormal events that are reasonably recoverable without widespread impact;
    - A centralized repository of shared cybersecurity information

As part of the general recommendation for greater educational resources, the subcommittees strongly support the establishment and use of ISAOs. These would help protect both traditional and non-traditional critical infrastructure sectors, by providing improved situational awareness to stakeholders. Information received through ISAOs may be used in real time to avert cyber threats. ISAOs would also be a path towards continuous collaboration and coordination with the DHS National Cybersecurity and Communications Integration Center, which coordinates cybersecurity information sharing amongst the federal government and the private sector.

At the council's Public Policy Forum on Cybersecurity in December 2016, Dr. Phyllis Schneck, then-DHS deputy under secretary for cybersecurity and communications for the NPPD, encouraged the Maryland Cybersecurity Council and the state to explore ways of enhancing information sharing between stakeholders. Dr. Schneck argued that information sharing was one of the most beneficial and cost-effective ways of increasing cybersecurity preparedness. DHS provides a free mechanism to support information sharing of which, she suggested, states should take advantage.

The Cyber Incident Response and Cyber Operations Subcommittee examined the role of the New Jersey Cybersecurity and Communication Integration Cell (NJCCIC) and noted its public facing, public safety focus as opposed to focusing solely on internal government networks. The NJCCIC provides businesses and citizens free access to forensics training and threat signatures, as well as coaching and mentoring to anyone or any business that is experiencing a cyber incident.

This subcommittee also looked at Arizona Infragard, a civilian organization whose members are vetted by the FBI, which serves as the backbone of Arizona's cyber public outreach. The 501C3 private public partnership provides training and cyber expertise to law enforcement, private citizens, and businesses. Born from a program sponsored by Johns Hopkins University Applied Physics Lab, this group is able to provide much more substantial incident response support to its members than the NJCCIC model.

Both subcommittees will pursue this recommendation by exploring structures that can expand situational awareness for the state, its critical infrastructure sector, and other businesses.

Cyber Operations and Incident Response Subcommittee

2017 Recommendation 9. The council recommends the implementation of a comprehensive Computer Network Defense (CND) program to provide robust protection to state assets, business information, and citizen data across all agencies. This program must prioritize the efforts to thwart multiple threats arrayed against the state.
The cyber threats to Maryland and its citizens have challenged the ability of state agencies to independently protect themselves. This was a major impetus behind the governor's initiation of an enterprise approach as recommended by the DoIT secretary. To improve the state's overall cybersecurity posture requires much greater investment. A modern defensive posture requires planned and well-executed investments that combine to provide the best defensive effect for the dollar spent.

The state's CND capability at present is recent and limited. In the 18 months since this capacity has operated, the world has experienced a great number of cyber firsts: Russia openly attacked a Ukraine power grid using malware that is now free to anyone with an internet connection; the North Koreans leveraged security lapses in international banking systems and were able to take hundreds of millions from sovereign governments; Russia used national assets to spy on a US election and attempted to influence its outcome; and an exploit directed at internet infrastructure simultaneously by millions of IoT devices interrupted internet service across the nation. The pandemic of ransomware has been astonishingly successful. One security firm reports that the reported number of global ransomware attacks in 2016 were 167 times greater than the number in 2015 (3.8 million reported attacks in 2015 versus 638 million attacks reported in 2016).[42]

Maryland is likely to be a higher target of interest not only to criminals but also to nation states given that many of its citizens work in defense and national security establishments located in the state and nearby Washington DC. A comprehensive cybersecurity program is a direct contributor to the state's ability to secure confidential citizen data, to meet its public safety mission, and to ensure reliable and effective state government operations. The full analysis of the subcommittee has been included to capture additional details supporting its recommendations.[43]

VI. Conclusion

Maryland has been a leader in mobilizing public and private stakeholders to examine and address cybersecurity issues confronting the state and its citizens. This report documents the Maryland Cybersecurity Council's contribution to this effort over the past two years and describes the council's agenda for the next two. Its work will be to develop proposals to implement its recommendations and to engage the many policymakers and other stakeholders who are the essential partners in advancing Maryland's cybersecurity.

[42] SonicWall 2017 Annual Threat Report at https://www.sonicwall.com/docs/2017-sonicwall-annual-threat-report-visual-summary-ebook-121934.pdf
[43] Appendix C

VII. Further Information

Questions about this report may be addressed to:

University of Maryland University College
ATTN Maryland Cybersecurity Council Staff
3501 University Boulevard East
Adelphi, Maryland 20783
Marylandcybersecuritycouncil@umuc.edu

APPENDIX A

Maryland Cyber Security Council Members by Sector

Maryland Cybersecurity Council

Chair
Attorney General Brian Frosh

Legislative Representatives
Senator Susan C. Lee
Senator Bryan W. Simonaire
Delegate Ned Carey
Delegate Mary Ann Lisanti

Cybersecurity Companies
John M. Abeles
President and CEO
System 1, Inc.

James Foster
CEO
ZeroFox

Zuly Gonzalez
Co-Founder and CEO
Lightpoint Security

Belkis Leong-Hong
Founder, President, and CEO
Knowledge Advantage, Inc.

Rajan Natarajan
President
TechnoGen, Inc.

Jonathan Powell
Senior Director, Software Engineering
General Dynamics Information Technology

Business Associations

Jim Dinegar
President and CEO
Greater Washington Board of Trade

Don Fry
President and CEO
Greater Baltimore Committee

Brian Israel
Business Development Executive
Maryland Association of Certified Public Accountants

Joe Morales, Esq.
Attorney
Maryland Hispanic Chamber of Commerce

Higher Education

David Anyiwo, PhD
Professor and Chair, Department of Management Information Systems
Bowie State University

Shiva Azadegan, PhD
Director, Computer Science
Towson University

Anton Dahbura, PhD
Executive Director, Information Security Institute
Johns Hopkins University

Stewart Edelstein, PhD
Executive Director
Universities at Shady Grove

Michael Greenberger
Director, Center for Health and Homeland Security
University of Maryland Francis King Carey School of Law

Anupam Joshi, PhD
Director, Center for Security Studies
University of Maryland, Baltimore County

Higher Education (Continued)
Jonathan Katz, PhD
Director, Cybersecurity Center
University of Maryland, College Park

Carl Whitman
Vice President of Instructional and Information Technology and Chief Information Officer
Montgomery College

David Wilson, EdD
President
Morgan State University

Crime Victim Representative

Sue Rogan
Director of Financial Education
Maryland CASH Campaign

Susceptible Industries

Jayfus Doswell, PhD
Founder, President, and CEO
The Juxtopia Group, Inc.

Kristin Jones Bryce
Vice President of External Affairs
University of Maryland Medical System

Joseph Haskins Jr.
Chairman, President, and CEO
Harbor Bank

Clay House
Vice President of Architecture, Planning, and Security
CareFirst

Peegen Townsend
Vice President of Government Affairs
Medstar Health

State Institutions

Acting Secretary Michael Leahy
Maryland Department of Information Technology

David Engel
Director
Maryland Coordination and Analysis Center

State Institutions (Continued)
Tami Howie
CEO
Maryland Tech Council

Ronald Kaese
Director of Federal Programs
TEDCO

Major General (MG) Linda Singh
Adjutant General of Maryland
Maryland Military Department

Anthony Lisuzzo
Board Member
Army Alliance

Walter “Pete” Landon
Director
Governor's Office of Homeland Security

Ken McCreedy
Senior Director, Aerospace and Cybersecurity
Maryland Department of Commerce

Colonel. William Pallozzi
Maryland Secretary of State Police

Russell Strickland
Director
Maryland Emergency Management Agency

State Institutions (Continued)
Steven Tiller
President
Fort Meade Alliance

Federal Institutions

Donna Dodson
Director, National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Judith Emmel
Associate Director for State, Local, and Community Relations
National Security Agency

Other Designees

Mark Augenblick, Esq.
Attorney
Pillsbury Winthrop Shaw Pittman LLP

Robert W. Day Sr.
Senior Security Monitoring Analyst
AECOM, Inc.

Howard Feldman, Esq.
Attorney
Whiteford, Taylor & Preston

Larry Letow
President and CEO
Convergence Technology Consulting

Blair Levin
Nonresident Senior Fellow, Metropolitan Policy Program
Brookings Institution

Henry J. Muller
Director of Communications-Electronics Research, Development and Engineering Center (CERDEC)
U.S. Army, Aberdeen Proving Ground (APG)

Other Designees (Continued)
Jonathan Prutow
Policy and Planning Business Analyst
Macro Solutions

Paul Tiao, Esq.
Attorney
Hunton & Williams

APPENDIX B

Maryland Cybersecurity Council Repository

Resources Identified by the

Critical Infrastructure and Cybersecurity Framework Subcommittee

General Resources Related to Critical Infrastructure (CI)			
Title	**URL**	**CI**	**Summary**
Cybersecurity Framework			
NIST Cybersecurity Framework	https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf	All	Lists of Functions, Categories, Subcategories, and Informative References for cybersecurity considerations for critical infrastructure
Executive Order 13636 – Improving Critical Infrastructure Protection	http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf	All	
Relevant Infrastructure Cybersecurity Standards/Plans			
NIST Cybersecurity Standards-Index	http://csrc.nist.gov/publications/PubsSPs.html#800-30	All	Reference to multiple NIST cybersecurity standards/guidelines.
North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards; CIP-002-5.1a: Cyber Security — BES Cyber System Categorization; CIP-003-6: Cyber Security - Security Management Controls ; CIP-004-6: Cyber Security - Personnel & Training ; CIP-005-5: Cyber Security - Electronic Security Perimeter(s) ; CIP-006-6: Cyber Security - Physical Security of BES Cyber Systems; CIP-007-6: Cyber Security - System Security Management; CIP-008-5: Cyber Security - Incident Reporting and Response Planning; CIP-009-6: Cyber Security - Recovery Plans for BES Cyber Systems; CIP-010-2: Cyber Security - Configuration Change Management and Vulnerability Assessments; CIP-011-2: Cyber Security - Information	http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx	Power (supply/ distribution)	Various cyber-security requirements by NERC. All of these are subject to enforcement upon power companies by NERC, which is the self-regulating organization for power companies.

Protection; CIP-014-2: Physical Security			
US Department of Homeland Security, Critical Infrastructure Resources	https://www.dhs.gov/critical-infrastructure-resources	All	A wide array of free tools and resources to government and private sector partners to enable the critical infrastructure security and resilience mission
US Department of Homeland Security National Infrastructure Protection Plan	https://www.dhs.gov/national-infrastructure-protection-plan	All	Outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.
Federal Emergency Management Agency (FEMA) ready.gov	https://www.ready.gov/	All	Provides resources on how individuals and businesses can be more prepared for an emergency
US Department of Homeland Security, Infrastructure Visualization Platform	https://www.dhs.gov/infrastructure-	All	A data collection and presentation medium that supports critical

	visualization-platform		infrastructure security, special event planning, and responsive operations.
US Department of Homeland Security, Enhanced Critical Infrastructure Protection	https://www.dhs.gov/ecip	All	An ECIP visit, conducted by Protective Security Advisors (PSAs) with critical infrastructure facility representatives: Establishes and enhances the DHS relationship with critical infrastructure owners and operators. Informs them of the importance of their facility. Explains how their facility or service fits into its specific critical infrastructure sector. Provides an overview of the Office of Infrastructure Protection (IP) resources available to the facility to enhance security and resilience. Reinforces the need for continued vigilance.
US Computer Emergency Response Team (CERT) C^3 Voluntary Program	https://www.us-cert.gov/ccubedvp	All	assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework)
US Department of Homeland Security Private Sector Resources Catalog	https://www.dhs.gov/private-sector-resources-catalog	All	Collects the training, publications, guidance, alerts, newsletters, programs, and services available to the private sector across the Department.

US Computer Emergency Response Team (CERT) Assessments: Cyber Resilience Review (CRR)	https://www.us-cert.gov/ccubedvp/assessments	All	a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
US Department of Homeland Security, National Infrastructure Protection Plan	https://www.dhs.gov/national-infrastructure-protection-plan	All	Overview of Strategic Planning, Risk Modeling, Analysis, and Assessment performed by DHS
US Department of Homeland Security, National Strategy for the Physical Protection of Critical Infrastructure and Key Assets	https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf	All	
National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge Fact Sheets	https://www.dhs.gov/publication/nipp-challenge-fact-sheets	All	Fact sheets for the National Infrastructure Protection Plan (NIPP) Security and Resilience Challenge
Paller, A., Testimony Before the House Committee on Homeland Security: Subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity, Hearings on SCADA and the Terrorist Threat: Protecting the Nation's Critical Control Systems	http://www.gpoaccess.gov/congress/index.html	Mostly Power	Information regarding vulnerability and risks of SCADA systems.
Business Continuity			
US Department of Homeland Security. Business Continuity Planning Suite	https://www.ready.gov/business-continuity-planning-suite	All	Program that discusses how to create Business Continuity and Disaster Recovery Plans
Federal Information System Security Plan Requirements			
NIST Special Publication 800-18: Guide for Developing Security Plans for Federal Information Systems	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf	All	Includes information on how to set up a System Security Plan. Although for federal systems, this could be adopted for infrastructure IT systems as well. Also includes technical controls and discusses risk analysis
Committee on National Security Systems, (CNSS), National	https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Infor	All	Glossary for common use of cybersecurity terms

Information Assurance (IA) Glossary	mation_Assurance.pdf		
NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf	All	
NIST SP 800-70, Security Configuration Checklists Program for IT Products - Guidance for Checklists Users and Developers	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r3.pdf	All	A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected.
Additional Materials			
Booz Allen Hamilton - When the Lights Went Out: A comprehensive review of the 2015 attacks on Ukrainian Critical Infrastructure	https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf		
NIST Internal/Interagency Report (NISTIR) 7621 - Small Business Information Security: The Fundamentals	http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf		
US Department of Homeland Security - Emergency Services Sector Cyber Risk Assessment	https://www.dhs.gov/sites/default/files/publications/Emergency-Services-Sector-Cyber-Risk-Assessment-Fact-Sheet-508.pdf		

US Department of Homeland Security - Strategic Principles for Securing the Internet of Things (IoT)	https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
Congressional Research Services (CRS) Report - Encryption: Frequently Asked Questions	https://www.everycrsreport.com/reports/R44642.html
East West Institute - A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets	https://www.eastwest.ngo/sites/default/files/A%20Measure%20of%20Restraint%20in%20Cyberspace.pdf
US Department of Homeland Security - Cyber and Infrastructure Protection Transition Way Ahead Report to Congress	http://www.steptoecyberblog.com/files/2016/04/Cyber-and-Infrastructure-Protection-Transition-Way-Ahead.pdf
US Senate Homeland Security and Government Affairs Committee Report: The Federal Government's Track Record on Cybersecurity and Critical Infrastructure	To be provided as pdf for the repository.
Food and Drug Safety and Innovation Act (DASIA) Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework	https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf
US Department of Energy Report: Energy Sector Cybersecurity Framework Implementation Guidance	https://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf
Financial Industry Regulatory Authority (FINRA): Report on Cybersecurity Practices	https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
Congressional Research Services (CRS) Report - Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis	https://www.everycrsreport.com/files/20150603_R43821_b38e90bc477145dccb26b78a82188cd443de4661.pdf

Previous Critical Infrastructures Risk Assessments			
Title	**Year**	**URL/location**	**Summary**
U.S. Department of Homeland Security: U.S. Critical Infrastructure 2025: A Strategic Risk Assessment	2016	https://info.publicintelligence.net/DHS-OCIA-CriticalInfrastructure2025.pdf	US DHS/Office of Cyber and Infrastructure Analysis assesses that the Healthcare and Public Health, Emergency Services, Transportation Systems, Water and Wastewater Systems, and Energy (Electrical Power) Sectors are most likely to be affected by a pandemic. All other critical infrastructure sectors are likely to be affected to some degree by the unavailability of personnel needed to maintain operations. The economic impact of a pandemic will depend on its severity and duration and mitigation efforts by federal, state, and local governments and the public. Estimates of loss in gross domestic product during the first year of a pandemic range from less than 1 percent in a mild pandemic up to 4.25 percent during a severe pandemic.
Joint Research Centre (JRC) Technical Notes: Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art	2012	https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf	Risk assessment procedures and recommendations for critical infrastructure. Although this is for the European Union, it could easily be tailored to needs for

			the US.
Risk analysis of critical infrastructures	Multiple	https://www.klima-umwelt.kit.edu/english/297.php	Links to resources associated with risk analyses of different critical infrastructures (you'll have to use google translate to translate some of the webpages)
US Department of Homeland Security - Strategic National Risk Assessment	2011	https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf	Strategic national risk assessment to help identify the types of incidents that pose the greatest threat to the Nation's homeland security. Much of the report is classified, so it is not available here.
North American Electric Reliability Corporation (NERC), Electric Reliability Organization (ERO) Enterprise Inherent Risk Assessment Guide	2014	http://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/ERO_Enterprise_Inherent_Risk_Assessment_Guide_20141010.pdf	Describes how power companies must perform risk assessments under NERC requirements
Joint Research Centre (JRC), Risk assessment methodologies for critical infrastructure protection. Part II: A new approach	2015	http://publications.jrc.ec.europa.eu/repository/bitstream/JRC96623/lbna27332enn.pdf	Risk analysis to various critical infrastructure performed for EU
Risk Analysis Models/Guides for Critical Infrastructure Systems			
NIST SP 800-30, Risk Management Guide for Information Technology Systems	2012	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf	Guide for conducting risk assessments for federal IT systems.
NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach	2010	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf	
Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems	2004	http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf	This publication establishes security categories for both information and information systems. The security categories are based on the potential

			impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems	2002	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf	Provides guidance for planning, establishing, maintaining, and terminating interconnections between information technology (IT) systems that are owned and operated by different organizations.
Risk Assessment Methodologies			
Risk and Vulnerability Analysis of Critical Infrastructures - The DECRIS Approach	2008	http://www.sintef.no/globalassets/project/samrisk/decris/documents/decris_paper_samrisk_final-080808.pdf	Method supports an "all hazards" approach across sectors; i.e., electricity supply, water supply, transport (road/rail), and information and communication systems (ICT). The end users of the method and decision support systems are local governments, municipalities, and companies responsible for the infrastructures. The objective of this paper is to present main features of the method and discuss some preliminary findings from the

			project's case study of Oslo municipality.
Scenario Based Approach for Risks Analysis in Critical Infrastructures	2015	http://iscram2015.uia.no/wp-content/uploads/2015/05/2-10.pdf	Presents a Cross-Impact Analysis methodology that can assist decision-makers and planners with analytical tools for modeling complex situations. These features are generally useful in emergency management and particularly within the critical infrastructures scope, where complex scenarios for risk analysis and emergency plans design must be analyzed
ISO 31000 International Standard: "Risk Management – Principles and Guidelines on Implementation"	2009	https://www.iso.org/standard/43170.html	Although ISO 31000:2009 provides generic guidelines, it is not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes, functions, projects, products, services, or assets and specific practices employed.
Risk Management Guide for Critical Infrastructure Sectors	2007	https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-	Discusses considerations for risk

		mngmnt-gd/index-en.aspx#_Toc267899983	assessment across critical infrastructures.
Congressional Research Service (CRS), The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress"	2014	https://fas.org/sgp/crs/homesec/RL33858.pdf	This report begins with an overview of the evolution of risk assessment methodologies from the Department of Justice in FY2002 to DHS in FY2007, and then discusses the discipline of risk management and risk assessment as applied to Homeland Security Grant Program (HSGP).
Model-based Risk Analysis For Critical Infrastructures	2015	https://www.witpress.com/elibrary/wit-transactions-on-state-of-the-art-in-science-and-engineering/54/23054	Discusses multiple risk analysis models for critical infrastructure
Critical Infrastructure Protection: DHS Action Needed to Enhance Integration and Coordination of Vulnerability Assessment Efforts	2014	http://www.gao.gov/assets/670/665788.pdf	Discusses various tools that DHS has to perform risk assessments for critical infrastructure and the short-comings of these tools
US Department of Homeland Security, Supplemental Tool: Executing A Critical Infrastructure Risk Management Approach- A guide for companies and government authorities	2013	https://www.dhs.gov/sites/default/files/publications/NIPP-2013-Supplement-Executing-a-CI-Risk-Mgmt-Approach-508.pdf	A useful critical infrastructure risk management approach, which supports the risk management framework
Protecting Critical Infrastructures – Risk and Crisis Management	2008	https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Protecting-Critical-Infrastructures.pdf?__blob=publicationFile	The guide is addressed to operators of critical infrastructures and is intended to help them create and expand their own systems of risk and crisis management

J. Johansson, L. Svegrup & H.Hassel, Societal Consequences of Critical Infrastructure Vulnerabilities	2014	https://books.google.com/books?id=u1DvBQAAQBAJ&pg=PA2027&lpg=PA2027&dq=risk+analysis+of+critical+infrastructures+which+one+most+risk&source=bl&ots=nzNN4DwjWa&sig=drEEhTMkYHQfJsVnd1VfCsjpUb0&hl=en&sa=X&ved=0ahUKEwjroca8l4bTAhUDkpAKHRwbAsM4ChDoAQg7MAY#v=onepage&q=risk%20analysis%20of%20critical%20infrastructures%20which%20one%20most%20risk&f=false	Integrated model for risk assessment including interdependencies among infrastructure sectors. Power is recognized as one of the most vital infrastructures
J. Johansoon, Risk & Vulnerability Analysis of Interdependent Technical Infrastructures	2010	http://www.iea.lth.se/publications/Theses/LTH-IEA-1061.pdf	Modeling approach based on dividing the model of the technical infrastructure into one structural and one functional part, enabling the analysis of interdependent technical infrastructures for both structural and functional strains. Empirical studies of electrical distribution systems and a railway system, consisting of seven interdependent subsystems, have been carried out to demonstrate the proposed modelling approach.
Using Risk Modeling, Analysis, and Assessment to Inform Homeland Security Policy and Strategy	2013	https://www.aferm.org/wp-content/uploads/2016/10/ERM_2013_Cohn_Using_Risk_Modeling.pdf	
US Department of Homeland Security, National Security Telecommunications Advisory Committee, National Security Telecommunications Advisory Committee (NSTAC) Task Force on Concentration of Assets: Telecom Hotels	2003	https://www.dhs.gov/sites/default/files/publications/Telecom%20Hotels_2.pdf	The Administration has expressed concern that the concentration of multiple entities' telecommunications assets in specific locations may have implications for the security and reliability of the

			telecommunications infrastructure. The President's National Security Telecommunications Advisory Committee (NSTAC) Industry Executive Subcommittee chartered the Vulnerabilities Task Force (VTF) to examine these issues. This report addresses the Administration's concerns about the concentration of telecommunications assets in telecom hotels.
Ted G. Lewis, Rudolph P. Darken, Thomas Mackin, & Donald Dudenhoeffer, Model-based Risk Analysis for Critical Infrastructures	2012	https://www.witpress.com/Secure/elibrary/papers/9781845645625/9781845645625001FU1.pdf	Describes a risk-informed decision-making process for analyzing and protecting large-scale critical infrastructure and key resource (CI/KR) systems, and a Model-Based Risk Analysis (MBRA) tool for modelling risk, quantifying it and optimally allocating fixed resources to reduce system vulnerability.

Critical Infrastructure (CI) Interdependencies				
Title	**Year**	**URL**	**Types of CI**	**Summary**
Interdependent Critical Infrastructure Systems	Multiple	https://www.ethz.ch/content/specialinterest/dual/frs/en/research/interdependent-systems.html	Communications technology (ICT), electric power supply, transportation, emergency (such as medical, rescue, fire and police), and financial services	The interconnectedness of these critical infrastructure systems also makes them vulnerable to disruptions of both internal and external nature. External factors include natural disasters, terrorism, and malicious behaviour of humans; while internal factors may include technical failures of components, systemic failures, and human errors.
Review on modeling and simulation of interdependent critical infrastructure systems	2014	http://www.sciencedirect.com/science/article/pii/S0951832013002056	Multiple	Modern societies are becoming increasingly dependent on critical infrastructure systems (CISs) to provide essential services that support economic prosperity, governance, and quality of life. These systems are not alone but interdependent at multiple levels to enhance their overall performance. However, recent worldwide events such as the 9/11 terrorist attack, Gulf Coast hurricanes, the Chile and Japanese earthquakes, and even heat waves have highlighted that interdependencies among CISs increase the potential for cascading failures and

				amplify the impact of both large and small scale initial failures into events of catastrophic proportions. To better understand CISs to support planning, maintenance and emergency decision making, modeling and simulation of interdependencies across CISs has recently become a key field of study.
Critical Infrastructure, Interdependency, and Resilience	2008	https://www.nae.edu/Publications/Bridge/EngineeringfortheThreatofNaturalDisasters/CriticalInfrastructureInterdependenciesandResilience.aspx	Highways, roads, bridges, airports, public transit, water supply facilities, wastewater treatment facilities, solid-waste and hazardous-waste service, agriculture and food systems, the defense-industrial base, energy systems, public health and health care facilities, national monuments and icons, banking and finance systems, drinking water systems, chemical facilities, commercial facilities, dams, emergency services, nuclear power systems, information	The concept of a "lifeline system" was developed to evaluate the performance of large, geographically distributed networks during earthquakes, hurricanes, and other hazardous natural events. Lifelines are grouped into six principal systems: electric power, gas and liquid fuels, telecommunications, transportation, waste disposal, and water supply. Taken individually, or in the aggregate, all of these systems are intimately linked with the economic well-being, security, and social fabric of the communities they serve.

			technology systems, telecommunication systems, postal and shipping services, transportation systems, and government facilities	
The Critical Interdependence of Our Infrastructure	2015	http://www.governing.com/blogs/view/gov-critical-interdependence-regional-infrastructure.html	Transportation, water, energy and waste systems	Whether across or within regions, however, one thing doesn't vary: Residents expect government leaders to keep their communities' infrastructure systems operating, and this entails spending a lot of money. In the Pacific Coast region alone, the West Coast Infrastructure Exchange estimates the need to be greater than $1 trillion over the next 30 years.
Critical Infrastructures and their Interdependence in a Cyber Attack – The Case of the U.S.	2015	http://www.inss.org.il/publication/critical-infrastructures-and-their-interdependence-in-a-cyber-attack-the-case-of-the-u-s/	Water, energy, transportation, emergency services, telecom, banking, government services, finance, business, information, oil & gas production & storage.	An attack on critical infrastructure is liable to have a decisive effect on the functioning of other infrastructures. The interdependence between infrastructures requires those involved in planning a cyber-attack as well as those involved in defending from such attacks to adjust to this reality and prepare accordingly. The article describes the existing models for

				analyzing interdependence between infrastructures, proposes an analytical framework for describing the interdependence and examines the possibilities at the United States' disposal should it decide to engage in a cyber-attack.
Post-Disaster Supply Chain Interdependent Critical Infrastructure System Restoration: A Review of Data Necessary and Available for Modeling	2016	http://datascience.codata.org/articles/10.5334/dsj-2016-001/	Transportation, power, communications, and water	Review what data are required for critical infrastructure interdependency model construction, the accessibility of these data, and their integration with each other.
Managing Critical Infrastructure Interdependence through Economic Input-Output Methods	2009	http://www.cmu.edu/gdi/docs/managing-critical.pdf	Water supply, oil, and gas distribution, power plants, telecommunication and transportation	An economic I-O analysis is used to estimate a broad class of critical infrastructure interdependencies including normal disruptions and natural hazards.
The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State of-the-Art	2006	https://www.scribd.com/document/258360989/The-Vulnerability-of-interdependent-Critical-Infrastructures-Systems	Electric power, gas and oil production and distribution, telecommunication, banking and finance, water supply systems, transportation, health care, emergency and government services, food supply	The focus on the cascading vulnerability shows that various levels of exposed elements can be considered within critical infrastructure systems, whose vulnerability depends on their level of dependency. Since vulnerability is also affected by time and geographical scale

				issues, these factors have been further analyzed, as the question of the definition of accurate parameters and indicators to express it. The conclusion highlights the necessity to adopt a holistic, multi-disciplinary approach to the vulnerability analysis of critical infrastructures systems
Modeling supply chain interdependent critical infrastructure systems	2015	http://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=3394&context=doctoral_dissertations	Transportation networks, electrical networks, a water system, communication networks, banking and finance sectors, emergency services	Interdependencies between the infrastructures are mapped to evaluate resiliency and a framework for quantifying interdependence is proposed. In addition, this work details the identification, extraction and integration of the data necessary to model infrastructure systems

APPENDIX C

Full Analysis of the Cyber Operations and Incident Response Subcommittee

Cyber Operations and Incident Response Subcommittee 2017 Final Report
Subcommittee Report submitted to the Maryland Cybersecurity Council
May 2, 2017

1.0 Forward

The Cyber Operations and Incident Response Subcommittee is pleased to present this Final Report to the Maryland Cybersecurity Council. This Report includes findings and recommendations developed over the past year and outlines the proposed activity for the next period.

The cyber threats arrayed against the state and the citizenry have generally eclipsed the ability of State agencies to independently protect themselves. This was a major impetus behind the Governor initiation of an enterprise approach as recommended by the DoIT Secretary.

We didn't get here overnight, as the saying goes, and to improve the state's overall posture requires much greater investment in cyber security. A modern defensive posture requires planned and well executed investments that combine to provide the best defensive effect for the dollar spent.

Meanwhile, the threat continues to change and evolve; the situation having now been exacerbated by criminals cheaply, easily and almost freely denying owners access to their own information, or posing as real characters in the middle of a normal financial transaction. One security firm catalogued 638 million ransomware attacks in 2016, *167 times more than in 2015*[44].

The members of the Committee were pleased to work in understanding, informing and ultimately, reducing the risk Marylanders face from malicious acts against the State's cybersecurity infrastructure.

2.0 Cyber Operations and Incident Response Subcommittee Members

- Chair: Michael Leahy, Acting Secretary, Maryland Department of Information Technology
- Walter Landon, Director, Governor's Office of Homeland Security
- Dr. Anupam Joshi, Director, Center for Security Studies, UMBC
- Delegate Mary Ann Lisanti, Maryland General Assembly
- Anthony Lisuzzo, Board Member, Army Alliance
- Robert W. Day, Sr., Senior Security Monitoring Analyst, AECOM, Inc.
- Kristin Jones Bryce, VP External Affairs, UMMS
- Colonel William Pallozzi, Maryland Secretary of State Police

[44] 2017 SonicWall Annual Threat Report

2.1 Subcommittee Objectives
The Subcommittee objectives were to build and then exercise a comprehensive cyber incident response plan, and to recommend how the State should monitor and assess 1) threats to the State's information technology assets and 2) the State's defensive posture. The Subcommittee explored ways in which the State could share situational information, build a common, comprehensible cyber picture, and share relevant cyber threat information as broadly as possible.

2.2 Subcommittee Approach to Achieving Objectives
To achieve its objectives, the Subcommittee first had to inventory and understand all of the assets currently employed against the problem.

The second task was to determine the best methodology to create an incident-management mindset around cyber defense and resilience, using existing organizational structures as much as possible to limit cost.

The third task was to identify 1) the technical structures necessary to inform the state of its cyber threat exposure, 2) how to share threat information widely, 3) how to determine agency risk tolerance, and, 4) how agencies can feed cyber information to a centralized, state-level security operations center.

The fourth task was to develop recommendations for building a best-of-breed State cyber protection and management program that would share threat information with citizens and businesses; informing efforts to build a public-private cooperative incident response capability; and incorporating cyber risk management within every state agency.

Lastly, the Subcommittee is working with Federal and State officials on the legal and appropriate use of the Maryland National Guard to help defend the state's networks and information technology assets. The cyber talent of the Maryland National Guard is unique in the nation, and effectively marshalling their capabilities could greatly assist the State's defense posture and overall resilience to a disruptive attack.

3.0 Subcommittee findings and recommendations
The Cyber Operations and Incident Response Subcommittee submits the following findings and recommendations:

3.1 Maryland Now Has a Comprehensive Plan to Ensure a Coordinated and Adaptable Response to and Recovery from a Cyber Attack
The *State of Maryland Cyber Disruption Contingency Plan* is a supplement to the *Consequence Management Operations Plan* (CMOP). It describes the strategy to coordinate State-level operations to support local, state, and Federal agencies in addressing potential or actual disruptions from a cyber-attack. The plan was first exercised cross-agency in April 2017, and was signed earlier this year. The Maryland Cyber Disruption Plan details are considered sensitive, but the Plan's basic structure is outlined in the attached slide deck at Appendix 1.

3.2 Development of Cyber Capabilities Recommended
The Subcommittee recommends developing cyber capabilities for

- Sharing cyber threat and incident-handling information
- Supporting public safety (cyber) infrastructures
- Providing outreach support for Maryland citizens and businesses to meet their cybersecurity challenges

3.2.1 Recommendation: Develop Capability for Sharing Cybersecurity Information and Providing Outreach Support

Thwarting cyber-attacks requires rapid sharing of information, from dozens of sources across any size network as well as across traditional "critical Infrastructure" silos (e.g., transportation, aviation, finance). Sorting through the thousands of threat signatures for the relevant threats to our networks, businesses, and citizens is a challenging and expensive task in terms of labor and equipment costs. After patching, automated information sharing and threat analytics development are foundational to an active defense.

3.2.2 Information-sharing and Outreach Example: New Jersey

The Subcommittee has examined the role of the New Jersey Cybersecurity and Communication Integration Cell (NJCCIC) and noted its public facing, public safety focus as opposed to focusing solely on internal government networks. The NJCCIC provides businesses and citizens free access to forensics training and threat signatures, as well as coaching and mentoring to anyone or any business that is experiencing a cyber incident.

3.2.3 Information-sharing and Outreach Example: Arizona

Arizona Infragard, a civilian organization whose members are vetted by the FBI, serves as the backbone of Arizona's cyber public outreach. The 501C3 private public partnership provides training and cyber expertise to law enforcement, private citizens, and businesses. Born from a program sponsored by Johns Hopkins University Applied Physics Lab, this group is able to provide much more substantial incident response support to its members than the NJ model.

3.2.4 Maryland recommendation, Restated

Maryland State government does not currently provide a service to Marylanders like either of these states. The Subcommittee recommends continued exploration of these concepts, and if deemed desirable, recommends state resources be expended.

The Subcommittee is also interested in developing public-private alliances similar in purpose to the Arizona and New Jersey models, and has sought expertise from the MD National Guard, the Department of the Treasury, and the Department of Commerce to further improve the State's public-facing cyber posture. From advertising the various cyber ranges in the state to improving workforce cyber education, a public-private alliance can also facilitate information sharing across industry or infrastructure silos as well as enhance overall public, state, and local government cyber security awareness.

Case 1, April 28, 2017: A user at a Maryland university was targeted in a classic phishing attack, and the user had unwittingly given up user credentials. Several systems were being altered by the attacker. A university Vice President, having limited incident response resources and no expertise in the domain, called the Director of Maryland Cybersecurity for assistance. Although the State does not maintain an operations center after business hours, a contract

incident-handler was identified and the incident was quickly brought under professional incident-handling.

There would normally be no record of the incident, no report required, no sharing of how the attack was manifested, and no learning.

We are also aware of cases where agency employees simply left their workstations and went home after they were notified by an attacker that their computer was being encrypted by ransomware — to the eventual detriment of a large segment of the network. The record here, too, is thin, undiscoverable except by those personally involved in the incident; this lack of information sharing severely limits the ability of the rest of government to learn from mistakes.

3.3 Recommendation: Implement a comprehensive Computer Network Defense (CND) program to provide robust protection to state assets, business information, and citizen data. This program must prioritize the efforts to thwart multiple threats arrayed against the state.

A comprehensive cybersecurity program is a direct contributor to the State's ability to meet its public safety and public service missions. By protecting confidential information under State stewardship and the information technology infrastructure undergirding it, a cybersecurity program helps ensure reliable and effective State government operations.

3.3.1 Requires a Shift in Funding Approach

Being proactive in the defense of state assets and monitoring the State's cybersecurity posture requires a shift in investment priorities within the state government. Traditionally, only a small percentage of the Department of IT's (DOITs) budget was dedicated to securing the devices DOIT was configuring for communications infrastructure and for one other agency. As DOIT has taken on a centralized IT role and shifted to working in an Enterprise context, the DOIT security budget and manpower have not kept pace.

The security function should, at minimum, be a percentage of the budgets of agencies served in the Enterprise and preferably, a percentage of the overall state budget. The Subcommittee recommends DOIT propose a state best-of-breed program, socialize that concept with the Council, and seek the resources necessary to achieve the cybersecurity posture all State agencies will be expected to maintain.

A best-of-breed program will be proposed in detail at the fall meeting of the Council, and will mark the initial transition of State Cybersecurity into a discrete state-wide activity as opposed to a single-agency responsibility. We expect the products to compete favorably for state resources.

3.3.2. Developing a Comprehensive Computer Network Defense (CND) Program

DOIT is 18 months into a limited cybersecurity improvement initiative, the main goal of which was to lay the groundwork for and initiate a comprehensive security program for the Maryland Executive branch.

3.3.3. Adoption of Center for Internet Security's (CIS) Critical Security Controls (CSC)

DoIT's comprehensive program addresses the cyber threats and explicitly assumes the risk where it is unable to achieve fidelity to the security standard as informed by the CIS Critical Security Controls. Also endorsed by the National Governor's Association, these controls are a concise, prioritized set of cyber practices created to thwart today's most pervasive and dangerous cyber-attacks.

The CIS Controls are developed, refined, and validated by a community of leading experts from around the world. Organizations that apply just the first five CIS Controls can reduce their risk of cyberattack by around 85 percent. Implementing all 20 CIS Controls increases the risk reduction to around 94 percent. The CIS Controls embrace the Pareto 80/20 Principle, the idea that taking just a small portion of all the security actions you could possibly take yields a very large percentage of the benefit of taking all possible actions.

The CIS Top 20 critical security controls are the de facto measurement and guide to implementing cybersecurity initiatives across a variety of industries. Importantly, implementing these security controls is the State's plan for achieving the goals expressed in NIST guidance.

- Lawmakers in California have defined cyber security due diligence in terms of a company's ability to demonstrate maturity against the CIS top 20 critical security controls.
- Likewise, many insurance carriers discount their cyber insurance rates to firms that demonstrate an ability to meet the mid-level or higher goals expressed by the CIS top 20 critical security controls

Figure 1 is a list of the CIS top 20 critical security controls and their relative overall importance to information security. Figure 2 maps DOIT's current security initiatives to the CIS top 20 critical security controls.

Figure 1: CIS Top 20 Critical Security Controls Effect on Attack Mitigation[45]

	Critical Control	Effect on Attack Mitigation
1	Inventory of Authorized and Unauthorized Devices	Very High
2	Inventory of Authorized and Unauthorized Software	Very High
3	Secure Configurations	Very High
4	Continuous Vulnerability Assessment and Remediation	Very High
5	Controlled Use of Administrative Privileges	High
6	Maintenance, Monitoring, and Analysis of Logs	High
7	Email and Web Browser Protections	High
8	Malware Defenses	Moderately High
9	Limitation and Control of Network Ports	Moderately High
10	Data Recovery Capability	Moderately High
11	Secure Configurations for Network Devices	Moderately High
12	Boundary Defense	Moderately High
13	Data Protection	Moderate
14	Controlled Access Based on Need to Know	Moderate
15	Wireless Access Control	Moderate
16	Account Monitoring and Control	Moderate
17	Security Skills Assessment and Training	Moderately Low
18	Application Software Security	Moderately Low
19	Incident Response and Management	Low
20	Penetration Tests and Red Team Exercises	Low

Figure 2: CIS Controls, ratings and current initiatives

CIS Critical Security Controls (CSC) Top 20	Rating- Oct 2016	State of Maryland CND Initiatives	Rating Apr 2017
CSC 1: Inventory of Authorized and Unauthorized Devices	xx%	Init 3: Asset Management Improvements	xx%
CSC 2: Inventory of Authorized and Unauthorized Software	xx%	Init 3: Asset Management Improvements	xx%
CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops,Workstations, and Servers	xx%	Init 7: System Security Baseline Improvements NEW - Init # - NAC	xx%

[45] "Applying the CIS Critical Security Controls to the Cloud", CloudPassage, 2016 via Information Systems Audit and Control Association

CSC 4: Continuous Vulnerability Assessment and Remediation	xx%	Init 4: Patch Program Improvements	xx%
CSC 5: Controlled Use of Administrative Privileges	xx%	Init 8 : Vulnerability Assessment Program Improvements Init 9: Security Operations Improvement & Expansion Init 10: Enterprise Onboarding Improvements	xx%
CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs	xx%	Init 9: Security Operations Improvement & Expansion	xx%
CSC 7: Email and Web Browser Protections	xx%	Init 5: Border Control Improvements	xx%
CSC 8: Malware Defenses	xx%	Init 6: Endpoint Protection & Response Improvements	xx%
CSC 9: Limitation and Control of Network Ports, Protocols, and Services	xx%	Init 5: Border Control Improvements NEW - Init # - NAC	xx%
CSC 10: Data Recovery Capability	xx%		xx%
CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	xx%	Init 5: Border Control Improvements	xx%
CSC 12: Boundary Defense	xx%	Init 5: Border Control Improvements	xx%
CSC 13: Data Protection	xx%	NEW - Init # - DLP	xx%
CSC 14: Controlled Access Based on the Need to Know	xx%		xx%
CSC 15: Wireless Access Control	xx%	NEW - Init # - NAC	xx%
CSC 16: Account Monitoring and Control	xx%	Init 9: Security Operations Improvement & Expansion	xx%

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps	xx%		xx%
CSC 18: Application Software Security	xx%		xx%
CSC 19: Incident Response and Management	xx%	Init 9: Security Operations Improvement & Expansion	xx%
CSC 20: Penetration Tests and Red Team Exercises	xx%		xx%

3.2.4 Changes in Threat, the Rationale for State Legislative Action:

In the 18 months since the limited CND program has operated, the world has experienced a great number of cyber firsts: Russia openly attacked a Ukraine power grid using malware that is now free to anyone with an internet connection[46]; the North Koreans leveraged security lapses in international banking systems and were able to take hundreds of millions from sovereign governments[47]; Russia used national assets to spy on a US election and possibly attempted to influence its outcome[48]; an exploit directed at internet structures simultaneous by millions of "Internet of Things" devices dropped internet service across the nation and disrupted something we'd long believed was invulnerable to attack[49]; the fortress that was Amazon Web Services crashed due to poor code management practices and all services, including those Maryland subscribes to, were unavailable for four hours or more[50]. The pandemic of ransomware has been astonishingly successful, security firm SonicWall reported 2016 attacks were 167 times the number in 2015 (638 million ransomware attacks reported in 2017)[51].

Maryland government and certainly our businesses and citizenry have endured the negative effects from all of these events. Still, Federal legislation does not appear imminent in any of these areas.

3.2.5 Potential Legislative Action

While the Federal Government continues to abstain from action, the Subcommittee would like Maryland to consider the following, though these are not the definitive recommendations of the committee or its members:

- Companies should attest that their products protect data against unauthorized access, and simply must implement two-factor authentication. State application developers should follow these security best-practices as well.

[46] Industrial Control Systems Cyber Emergency Response Team, DHS, Alert IR-ALERT-H-16-056-01
[47] Symantec was first to link North Korea to these thefts.
[48] Dr. Dmitri Alperovitch, Co-Founder and CTO, CrowdStrike, to the MD Cyber Council, March 2017
[49] US Computer Emergency Readiness Team, DHS, Alert TA16-288A
[50] USA Today, March 2, 2017
[51] 2017 SonicWall Annual Threat Report

- Power companies and medical device manufacturers are among the most critical and most dispersed interconnected information systems. Although they are regulated in many ways, their cybersecurity posture is generally assumed to be adequate. That could be a mistake, requiring a third party assessment should be mandatory for licensing.
- Jurisdiction in cybercrime is limited by State and National boundaries, but states could form regional alliances to help erase some of those boundaries, and could pursue cyber criminals more broadly and more easily.
- A federal breach law does not exist, but Maryland law is at the forefront of that effort. Any number of states could serve to inform a Federal model, which is desirable from a legal and regional response viewpoint.
- All the states together comprise a large procurement pool. States making IT purchases should restrict purchases to vendors who attest that their code and their implementations meet an independent, third-party security test. That requirement is already in place for businesses who want to write code for Boeing, Wells Fargo, and Aetna. Why not for Maryland and the States as a whole?

Case 2, April 14, 2017: Our federal partners notified states of a sophisticated attack on vendor letters of credit issued via SWIFT. We were able to reach out to the Treasury, make sure the message was received and they would notify their subscribers accordingly. No further intelligence has been developed nor has a Maryland victim emerged. Of note, we were able to confirm that states bordering Maryland were also aware of the threat.

Cyber threats emerge in new places from new tools; sometimes the actors have tacit national and state approval if not support, and costs are rising. To say it's a team effort to defeat these threats understates the case. Cyber defense requires governments, citizens, and businesses to conduct their affairs in a collaborative, secure manner, or choose not to conduct that business until they can meet a minimum cybersecurity standard.

Maryland's relatively young cyber program, resourced wholly from within the Department of IT, is very young as far as determining and impacting the overall State cybersecurity posture. The program has run into a critical challenge posed on the one hand by a broad and growing threat active against the State and the citizenry, and on the other hand the limited scope of DOIT's historical mission and resource profile. Locked into a single agency's budget limitations, and competing for top-tier talent from within DOITs limited resource pool, the CND Program has not been able to expand rapidly enough to effectively meet to the threat.

4.0 Select Notes from the Security Case Log, for Security Awareness

- Our open, interconnected businesses and preference for sharing information across multiple social media platforms are being exploited by criminals and criminal gangs, actors who are mostly beyond the reach of state or federal legal jurisdictions. Maryland government is equally targeted by these actors, and they are having success.

  Case 3, March 14, 2017: A state procurement official's email was mimicked and used to send a request to every vendor she did business with. That message asked each targeted vendor to "test a banking connection" by depositing $2,000. The destination account was

an out-of-state bank, and header analysis showed the criminal was likely operating from Russia.

The FBI categorizes business email compromise as the fastest growing threat vector, illegitimately harvesting over $3B last year world-wide. In general, an errant banking transfer becomes unrecoverable after 24 hours.

Strengthening email security profiles, implementing anti-spoofing techniques, and implementing web service "anti-scraping" features are critical technical controls to combat these attacks.

Training of both the government executives who are most likely to become unwitting characters in the scheme as well as our business partners and citizenry is crucial to limiting the success of these attacks.

- The pandemic outbreak of ransomware has been the largest generator of cybercrime dollars annually for the last two years, yet was a very unlikely threat as few as five years ago. For as little as $20,000, criminals can buy sophisticated tools and even subscribe to Cloud Ransomware as a Service. Their targets include every citizen, business, and government entity. As in the case with business email compromise, ransomware criminals often reside and operate offshore, sometimes with the tacit approval of their resident nations.

  Case 4A, Thanksgiving Day, 2016: A Maryland county e911 operator noticed his computer was acting incorrectly and immediately disconnected it from the county network. The ransomware had already infected major parts of the network, however, and severely curtailed government's ability to function. Restoration of basic government functions took four days, with full restoration taking more than four months.

  Although the FBI says, "Never pay" in public, many entities capitulate to the criminal — police departments, dentists, hospitals and citizens simply comply with the demand. Of course, if they do not make changes to their protective posture, they'll likely be hit again, having been tagged in the criminal underworld as a victim who is quick to pay or an easy mark.

  Ransomware can generally be prevented by regular patching of deployed hardware and software. Diligent attention to the first five critical security controls as well as email security enhancements can prevent this type of infection from being successful.

  In the event ransomware does take hold, proper security protocols, quickly employed, proper backup and recovery procedures, as well as proper user and network segmentation will inhibit the ability of the ransomware to spread and will greatly ease clean up and forensic analysis.

In the above case, our CND security engineers were able to analyze the attack and limited the damage by deriving the criminal's own encryption key. Still, many of the infected assets were not recoverable and required a complete rebuild.

Case 4B, November 28th, 2016: The ransomware event that incapacitated our county government sounded similar to press reports coming out of the San Francisco Municipal Transit Authority. Rail service was curtailed. A Cyber Intelligence Analyst at the Maryland Coordination and Analysis Center noted the similarity, made phone calls, and shared our county story with authorities in California. Inspection showed the attack was likely from the same criminal; the decryption key we derived worked for them as well.

5.0 Conclusion

We believe the State is well served with the addition of the cyber incident response plan to the Maryland Emergency Management Agency's other Critical Infrastructure plans. We also note that the State plan required very little re-work to fit within the framework used by the National Cyber Incident Response Plan, published in January, and believe that speaks to the overall strength of the plan. Through exercising the components of the plan, the plan will be updated and revised in accordance with MEMA change-management procedures.

Looking forward, expanding both information sharing and security monitoring services are going to be vigorously explored, preferably in the context of a public-private partnership, or an alliance of state, local, and public entities.

A comprehensive security program, properly resourced and organizationally sustainable, should be considered a paramount goal for the State to achieve in the near term.

The Subcommittee is pleased to submit this Report to the Maryland Cybersecurity Council.