Maryland Cybersecurity Council Activities Report 2017 – 2019

July 1, 2019

TABLE OF CONTENTS

I. Statutory Requirement

This is the second biennial activities report of the Maryland Cybersecurity Council covering FY 2018 and 2019. The report is required by SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 (k).[1] All Council reports, the Council's membership, its plenary and subcommittee meeting minutes, and various cybersecurity resources for critical infrastructure owners and operators, consumers and small- and medium-size businesses may be found on the Council's website at http://www.umuc.edu/mdcybersecuritycouncil.

II. Activity Highlights

To date, the Council has made 26 recommendations.[2] These have focused on a range of issues, including consumer protection, workforce development, the level of State government investment in its cybersecurity, the security-related needs of critical infrastructure owners and operators, and small and medium-size businesses, among others. In the last two years, the objectives of a number of these recommendations have been realized, either through the Council's legislative members or in other ways. The chief outcomes are highlighted below. Section V of this report includes a fuller discussion of Council-related activities.

Legislation

The Council's membership includes four members of the General Assembly: Senator Susan Lee (District 16), Senator Bryan Simonaire (District 31), Delegate Ned Carey (District 31A), and Delegate MaryAnn Lisanti (District 34A). In the 2017-2019 period, these four legislative members sponsored seven bills[3] that were consistent with the objectives of various Council recommendations. Other members of the Council supported their efforts by offering favorable testimony in committee.[4] In three cases, bills were enacted during the 2018 session: SB 202/HB 710 (Chapters 676 and 677, Acts 2018, effective October 1, 2018), SB 553 (chapter 467, Acts 2018, effective July 1, 2018) and SB 204 (Chapter 415, Acts 2018, effective July 1, 2018):

- SB 202/HB 710 (Consumer Protection – Credit Report Freezes – Notice and Fees). Sponsored by Senator Lee and Delegate Carey, the law prohibits any of the credit reporting agencies from charging affected consumers a fee for the placement, removal, or temporary lift of a security freeze. The Act built on SB 270/HB 212 (also sponsored by Senator Lee and Delegate Carey) that passed in the 2017 session and prohibited fees for initiating a credit freeze after notification of being affected by a breach. The purpose of

[1] Section k states that "beginning July 1, 2017, and every two years thereafter, the Council shall submit a report of its activities to the General Assembly in accordance with § 2–1246 of this article".
[2] See Appendix A to this document for the recommendation synopses. For details, see the Council's *July 1, 2016 Initial Activities Report* and its *July 1, 2017, Activities Report* at http://www.umuc.edu/mdcybersecuritycouncil
[3] Cross-files are counted as one bill.
[4] These included Mr. Markus Rauschecker, Dr. Jonathan Katz, Mr. Patrick Feehan, Dr. Anton Dahbura, and Dr. Kevin Kornegay, all representing themselves in their Council roles.

the Council's underlying recommendation[5] and both statutes is to encourage consumers to be proactive in protecting their identities when notified of a breach involving their personal identifying information.

- SB 553 (State Government - Security Training - Protection of Security-Sensitive Data). Sponsored by Senator Simonaire, the statute requires that all units of State government develop a plan and execute training for employees handling "security sensitive" information held on organizations and private citizens. The State Department of Information Technology (DoIT) had been offering such training to agencies. The effect of the bill, which became law on June 1, 2018 and also included certain reporting requirements, is to mandate that all agencies of State government participate in the training. As an incremental step, the bill furthers the objectives of the Council's 2017 recommendation calling for the State to enhance its cybersecurity posture.[6]

- SB 204 (Cybersecurity Public Service Scholarship Program). Sponsored by Senator Simonaire and Senator Lee, the law establishes a cybersecurity scholarship-for-service program. In return for each year of scholarship support, program graduates must complete a one-year obligation within a unit of State government in a cybersecurity work role or teach in a public high school in a curriculum directly related to cybersecurity. The law answered a Council recommendation calling for such a program to help alleviate the talent shortfall in cybersecurity.[7] In its first year, 190 applications for the scholarship were received. The program was funded at $160,000 in FY 2019 and will remain at that level in FY 2020.

Non-legislative Council Activities.

- In December 2017, the Council launched a web-based searchable repository with free, curated resources on cybersecurity for critical infrastructure owners and operators as well as small- and medium-size businesses, and consumers.[8] This realized a recommendation to make it easier for these constituencies to access practical information by filtering the many resources generally available and hosting them online in one place.[9]

- The Council scheduled a number of briefings at its plenary meetings on the State government's cybersecurity needs. The Council also benefited from a report of the Subcommittee on Cyber Operations and Incident Response. The objective of this effort was to quantify the fiscal effort that might be required for the DoIT to implement a mature computer network defense program.[10] As an outcome, the Council endorsed a resolution at its October 25, 2017, meeting urging an investment of $28.9 million dollar

[5] See Appendix A, 2016 Recommendation 4.

[6] Appendix A, 2017 Recommendation 9. For more details, see the background discussion informing Recommendation 9 in the *July 1, 2017 Activities Report* (Appendix C) at http://www.umuc.edu/mdcybersecuritycouncil

[7] Ibid., 2016 Recommendation 11.

[8] The repository may be found at http://www.umuc.edu/mdcybersecuritycouncil

[9] Ibid., 2016 Recommendation 8.

[10] Ibid., 2017 Recommendation 9.

in DoIT's cybersecurity function with an annual, inflation-adjusted sustainment budget of $14 million to $15 million thereafter.

- Not responsive to a recommendation of record but recognizing the present ransomware emergency in Baltimore City, the Council approved a resolution at its May 22, 2019, meeting encouraging members to volunteer their expertise to the special security committee convened by Baltimore City Council President Brandon Scott. Five Council members, all faculty of Baltimore-area schools, responded to the call and were subsequently identified to Mr. Scott in a letter representing the Council.[11] As the staffing agency for the Council, University of Maryland Global Campus also notified the City of two of its faculty willing to volunteer their time and expertise.[12]

- As an ongoing outreach initiative, the Council has continued to organize an annual reception in Annapolis at the beginning of session with subject matter experts to discuss cybersecurity issues for legislators and their staff members. The Council's January 2018 reception included Deborah Plunkett, former director of the NSA's Information Assurance Directorate and a Senior Fellow at Harvard University's Belfer Center for Science and Technology. The 2019 speaker was Lt. General Harry Raduege Jr. (USAF, Ret), former Director of the Defense Information Systems Agency (DISA) within the US Department of Defense.

Other Developments of Note

The recommendations of the Council reflect concerns that in many cases are broadly shared, and accordingly it is important to note efforts of others apart from the Council that are addressing those concerns. These include laws sponsored by other legislators (2018 HB 281 and 2018 SB 228)[13] and initiatives launched within the executive branch as a result of the Governor's October 2017 and June 2019 executive orders on cybersecurity.[14] These are discussed in Section VI below.

III. The Council's Mission, Organization, and Membership

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

[11] Dr. Anthony Dahbura, Executive Director, Johns Hopkins University Information Security Institute; Mr. Michael Greenberger, Professor of Law, and Director, Center for Health and Homeland Security, Francis King Carey School of Law; Dr. Anupam Joshi, Professor of Computer Science, University of Maryland Baltimore County; Dr. Kevin Kornegay, Professor and Endowed IoT Chair, Electrical and Computer Engineering Department, Morgan State University; Mr. Markus Rauschecker, Cybersecurity Program Director, Center for Health and Homeland Security, Francis King Carey School of Law.

[12] Mr. Daniel Mintz, Program Chair, Information Systems Management, and Collegiate Associate Professor, and Mr. Bruce DeGrazia, Program Chair, Cybersecurity Management and Policy, and Collegiate Professor.

[13] Chapters 358 and 528, respectively, Acts 2018, effective June 1, 2018.

[14] Executive Orders 01.01.2017.22, October 5, 2017 and 01.01.2019.07, June 18, 2019, accessed at https://governor.maryland.gov/category/executive-orders/

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.[15]

By statute, the Council is chaired by the Attorney General or the Attorney General's designee.[16] It currently consists of 57 other members organized into six subcommittees. The Council's composition reflects a 'whole of community' approach to addressing cybersecurity issues.[17] 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.[18] In 2018, the State Administrator for the State Board of Elections was added to the Council's membership as a result of legislation sponsored by Senator Simonaire.[19] 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 Council as a whole meets three times per year. As part of its ongoing discovery, it dedicates part of its business meetings to presentations by subject matter experts on cybersecurity-related issues. During 2017-2019, these included Mr. Rick Wilson, former Senior Intelligence Officer and Defense Intelligence Senior Leader at the National Security Agency; Mr. Bill Lawrence, Director, Energy-Information Sharing and Analysis Center (E-ISAC) and Senior Director, North American Electric Reliability Corporation (NERC); Ms. MaryAnn Tierney, Regional Administrator for Federal Emergency Management Agency (FEMA) Region III; and Mr. Eugene Kipniss, Senior Program Specialist at the Multi-State Information Sharing and Analysis Center (MS-ISAC).

In large measure, however, the Council's fact-finding and formulation of recommendations occurs within its subcommittees, which convened a total of 15 times during the two-year period. The subcommittees, their objectives and current appointed members are as follows.

Subcommittee on Law, Policy and Legislation

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

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

[16] Ibid, §9-2901 (G)

[17] Ibid, §9-2901(C)-(F)

[18] For members grouped by sector, see Appendix A.

[19] SB 281. MD. Ann Code, St. Gov't Art. §9-2901

Subcommittee Members

- Co-Chair: Susan C. Lee, Senator, District 16, Maryland General Assembly
- Co-Chair: Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution
- Ned Carey, Delegate, District 31A, Maryland General Assembly
- Howard Feldman, Esq., Attorney, Whiteford Taylor Preston
- 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

Subcommittee on Cyber Operations and Incident Response

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, Secretary of Department of Information Technology (DoIT)
- Kristin Jones Bryce, Senior Vice President of External Affairs, University of Maryland Medical System
- Robert W. Day Sr., Councilman, College Park, Maryland
- Judith Emmel, Associate Director, State, Local, and Community Relations, National Security Agency; liaison to the Council
- Terri Jo Hayes, Cybersecurity Strategist, mfusion, Inc.
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Fred Hoover, Esq, Attorney, Maryland Office of the People's Counsel
- Linda Lamone, Administrator, State Board of Elections
- Walter "Pete" Landon, Director, Governor's Office of Homeland Security
- Mary Ann Lisanti, Delegate, District 34A, Maryland General Assembly
- Anthony Lisuzzo for Tom Albro, President, Army Alliance
- Colonel William Pallozzi, Maryland Secretary of State Police

Subcommittee on Critical Infrastructure and Cybersecurity

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: Markus Rauschecker, Cybersecurity Program Director, Center for Health and Homeland Security, 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
- 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
- Michael Greenberger, Director, Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland, Baltimore
- Clay House, Vice President, Architecture, Planning, and Security, CareFirst
- Rajan Natarajan, CEO, QualityPro, Inc.
- Bryan Simonaire, Senator, District 31, Maryland General Assembly
- Major General Linda Singh, Adjutant General of Maryland, Maryland Military Department

Subcommittee on Education and Workforce Development

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
    - Attracting teachers and faculty qualified to teach cybersecurity courses in high school and beyond
    - 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, including recommendations on:
    - Funding for R&D
    - Incentivizing R&D
    - Collaborative R&D
- Recommendations on pathways to employment in the cybersecurity field

Subcommittee Members

- Chair: Jonathan Katz, PhD, Director, Maryland Cybersecurity Center and Professor, Department of Computer Science, University of Maryland, College Park
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove, 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
- Christine Ross, President and CEO, Maryland Chamber of Commerce
- Russell Strickland, Director, Maryland Emergency Management Agency
- Dr. Kevin Kornegay for David Wilson, EdD, President, Morgan State University

Subcommittee on Economic Development

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.
- Brian Corbett, Director Seed Investment, Maryland Technology Development Corporation (TEDCO)
- James Foster, CEO, ZeroFox
- Don Fry, President and CEO, Greater Baltimore Committee
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Brian Israel, Business Development Executive, MACPA
- Ken McCreedy for Kelly M. Schulz, Secretary, Maryland Department of Commerce
- Marty Rosendale, CEO, Maryland Tech Council

- Christine Ross, President and CEO, Maryland Chamber of Commerce
- Steven Tiller, Esq, for Doreen E Harwood, President, Ft. Meade Alliance

Subcommittee on Public Awareness and Community Outreach

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
- Patrick Feehan, Data Protection Officer and Interim Deputy CIO/Performance Management, Montgomery College
- Larry Letow, President, LG-Tek

Council Staffing

The University of Maryland Global Campus is the staffing agency for the Maryland Cybersecurity Council.[20] 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.

IV. The Context of the Council's Work

The Council's recommendations are not shaped in a vacuum. They originate in certain problems that our digitized and connected world present to Maryland citizens, businesses, and government. This is not to ignore or understate the many benefits that modern technology, communications, and related tools have produced. As the Federal Trade Commission has stated:

> These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play

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

> music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident….[21]

The Council's charter is simply an acknowledgement that with transformative technological developments, there are collateral effects that are usually unforeseen and require policies to address them. These effects are well known and include the following:

Ubiquitous victimology[22]. Nationally, the Privacy Rights Clearinghouse reports that in 2018 there were 1,366,471,618 records held by various organizations in the US that were breached. In 2017, the number of breached records was higher: 2,048,395,688.[23] The primary source of data are the reports made to the states attorneys general and the Department of Health and Human Services Office of Civil Rights.[24] In a given case, more than one record may correspond to an individual—e.g. different records for social security number and date of birth—so that that the number of records and individuals affected cannot be simply equated.

Nonetheless, the magnitude of breached data is staggering, and it is highly likely that a large number of US consumers were affected by multiple breaches within this two-year period. This is imaginable, for example, with the hacks at Equifax (145 million records), Facebook (50 million records), and Ticketfly (26 million records). Equally important, the data breached were not the same in these cases, likely broadening the exposure of personal information for some number of individuals: Equifax (social security numbers, drivers' license information, credit card numbers, and other tax ID information),[25] Facebook (complete access to user accounts and third-party apps like Instagram),[26] and Ticketfly (physical addresses, phone numbers, as well as other information).[27]

The national trends are certainly reflected in Maryland. In FY 2018, there were 4,049,531 reported cases of Maryland residents being affected by a breach.[28] Since these are separately reported cases, it is again highly likely that many Maryland residents were affected by more than

[21] Federal Trade Commission Staff Report, Internet of Things: Privacy and Security in an Interconnected World, January 2015, p. 2, accessed at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[22] This term was coined by Mary Aiken, *The Cyber Effect (*New York: Spiegel and Grau, 2016), Chapter 9.

[23] See Privacy Rights Clearinghouse at https://www.privacyrights.org/. The data reported here results from queries involving all breach types and all organizations.

[24] Email exchange between Council staff and the PRC database manager on April 11, 2019.

[25] See Aimee Picchi, "It's Been a Year Since the Equifax Breach. Is Your Data Any Safer?", Consumer Reports, September 8, 2018, at https://www.consumerreports.org/data-theft/equifax-data-breach-is-your-data-any-safer/.

[26] Richard Nieva, Laura Hautala, Alfred Neg, "Facebook breach put data of 50 million users at risk", CNET, September 18, 2018, at https://www.cnet.com/news/facebook-breach-affected-50-million-people/.

[27] Lorenzo Franceschi-Bicchierai, "Hacker Stole 26 Million Email And Home Addresses Of Ticketfly Users", *Motherboard*, June 4, 2018, at https://motherboard.vice.com/en_us/article/j5kd4b/ticketfly-hack-breach-26-million-users-emails-home-addresses.

[28] As is the case with all states now, Maryland requires qualified breaches involving Maryland residents to be reported to the Office of the Attorney General. These data are from the draft *2018 Maryland Data Breach Report* to be published on the Council's website. The data are derived the Maryland Information Security Breach Notices website: http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/breachnotices.aspx

one breach and that in some number of cases the cumulative effect was the compromise of more and more sensitive information:

FY 2018 Maryland Breach Snapshot[29]

Type of Personal Information Lost or Exposed	**Total Maryland Residents Reported As Affected in Breach Notices**	**# Organizations Involved**
Full social security number with at least name	3,575,046	446
Payment card information with other personal identifying information	140,807	193
Bank account number or other banking information with other personal identifying information	10, 349	41
Medical or treatment information with other personal identifying information	65,337	70

Complexity[30]. The Internet of Things (IoT) refers to "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment".[31] IoT devices themselves have been described as computers with sensors and other things attached to them:[32] the car is a computer with wheels, the connected refrigerator is a computer that keeps things cold, airplanes are computers that fly, and so forth. Other examples of IoT devices include connected light bulbs, wearables, medical implants, children's toys, and industrial control systems (ICS) remotely routing trains and electricity and controlling dams and water treatment facilities. One estimate is that Internet of Things devices will exceed 14 billion worldwide in 2019 and reach 25 billion by 2021.[33]

Without question, IoT has created new horizons for consumer convenience and has contributed significantly to economic efficiency. But like any technological development, it has also spawned a variety of concerns. One is the expansion in personally sensitive data that is captured and communicated over the internet. These data include geolocation, information about one's body, surveillance streams from home and business cams, viewing tracking by smart TVs, and conversations recorded by home assistants and connected children's toys. This creates a number of privacy risks traceable to the devices themselves, consumer practices, and the apps that IoT devices can host.

- Consumer practices and inherent device insecurity. Many devices have hard-wired passwords that can be found on the internet, exposing consumers to hacks. In other cases, the passwords are changeable, but consumers rely on the provided default or create passwords that are easily broken. An example of a password hack are the reports last year of compromises

[29] The data in this table are derived from the Maryland Information Security Breach Notices site.

[30] A common point uncommonly summarized in Bruce Schneier, *Click Here to Kill Everybody* (New York: WW Norton and Company, 2018), pp. 26-33.

[31] Gartner IT Glossary at https://www.gartner.com/it-glossary/internet-of-things.

[32] Schneier, opus cit, p.5.

[33] Frederick Paul, "Gartner's top 10 IoT trends for 2019 and beyond", *Networked World*, November 26, 2018, at https://www.networkworld.com/article/3322517/a-critical-look-at-gartners-top-10-iot-trends.html

involving a Nest cam baby monitor, discovered by the parents who overheard male voices talking to their infants.[34] But it is often the case that devices with audio and/or video capability can be hacked by circumventing passwords altogether. This has been demonstrated with connected vacuums, routers, video consoles, and other devices.[35] Attacks via IoT devices are expected to accelerate with the deployment of automated vulnerability finders by criminals and other actors.[36]

- The applications that run on IoT devices likewise offer many consumer conveniences but present their own privacy issues, namely, transmitting sensitive data often without disclosure and leaving users exposed to revealing breaches. One report describes how women's period-tracking app, Flo, used by 25 million women sent their data to Facebook without disclosure and with the unique device identifier. The report tested other apps with similar findings.[37] In another report, a children's smart watch with an app enabling parents to track them was found to easily allow a hacker both to locate and contact a child.[38] A study of medical apps—such as those to remind patients when to take medicine, to research pharmacies, and the like—concluded on the whole that there was a lack of transparency about data collection and inadequate efforts to secure consent.[39] Moreover, the researchers found that even when no personally-identifiable information is shared by the app, the "network positions of several companies who control the infrastructure in which apps are developed, as well as the data analytics and advertising services, means that users can be easily and uniquely identified, if not by name. For example, the semi-persistent Android ID will uniquely identify a user within the Google universe, which has considerable scope and ability to aggregate highly diverse information about the user."[40]

[34] Ms. Smith, "Hijacked Nest devices highlight the insecurity of the IoT", *CSO*, February 9, 2019, accessed at https://www.csoonline.com/article/3338136/hijacked-nest-devices-highlight-the-insecurity-of-the-iot.html. See also: Jana Kasperkevic, "Cayla, the connected doll, is a spy and must be destroyed", *Marketplace*, April 14, 2017, accessed at https://www.marketplace.org/2017/04/14/world/Cayla-connected-doll-spy-must-be-destroyed; and FBI Alert I-071717(Revised)-PSA, Consumer Notice: Internet-connected Toys Could Present Privacy and Contact Concerns for Children, July 7, 2017, accessed at https://www.ic3.gov/media/2017/170717.aspx

[35] Jeremy Kirk, "IoT Security Fail: Hacked Vacuum Cleaner Becomes Spy Cam", *Bank Info Security*, October 30, 2017, accessed at https://www.bankinfosecurity.com/iot-security-fail-roving-spying-vacuum-cleaner-a-10414; Lily Hay Newman, "A long-awaited IoT Crisis is Here, and Many Devices Are Not Ready", *Wired*, April, 9, 2019, accessed at https://www.wired.com/story/upnp-router-game-console-vulnerabilities-exploited/; and Waqas, "Smart home devices can be hacked within minutes through Google search", *Hack Read*, March 15, 2018, accessed at https://www.hackread.com/smart-home-devices-hacked-in-google-search/. For a security analysis of a connected light bulb noted by Bruce Schneier, see "Pwn the LIFX Mini white", *Limited Results*, January 23, 2019, accessed at https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/

[36]See Lilly Hay Newman, "A New Way to Track Down Bugs Could Help Save IoT", *Wired,* January 1, 2018, accessed at https://www.wired.com/story/a-new-way-to-track-down-bugs-could-help-save-iot/

[37] Sam Schechner and Mark Secada ,"You Give Apps Sensitive Personal Information. Then They Tell Facebook", *Wall Street Journal*, February 22, 2019, accessed at https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

[38] Lindsey O'Donnell, "A popular Australian smartwatch's tracking capabilities expose its user's locations, personal data and more", *Threatpost*, April 16, 2019, Accessed at https://threatpost.com/tictoctrack-smartwatch-flaws-track-kids/143791/ The watches referenced can be purchased on common ecommerce platforms in the US.

[39] Quinn Grundy, Kellia Chiu, Fabian Held, Andrea Continella, Lisa Bero, and Ralph Holz, "Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis", *BMJ*, March 20, 2019, accessed at https://www.bmj.com/content/bmj/364/bmj.l920.full.pdf, p. 10

[40] Ibid.

- While not a new issue, the ubiquity of IoT devices has increasingly sharpened the question of consumer control over who holds their data.[41] This data is monetized by using it for advertising and by selling it to third parties for aggregation with other information to form very detailed profiles of consumers' habits and preferences.[42] Access to these datasets are in turn sold to advertisers. The concentration of so much data creates additional risk for the consumer, since the cloud repositories become highly attractive targets for compromise.[43]

Beyond privacy considerations, the vulnerability of IoT devices has brought safety concerns. These go beyond the vulnerability of consumer devices to include connected medical implants,[44] automobiles,[45] and inflight airplanes,[46] among many other devices shown to be susceptible to hacks. Moreover, the very diffusion of IoT devices with poor security across all sectors of society allows them to be potentially weaponized.

Distributed Denial of Service (DDoS) attacks occur when the computing power of a large number of IoT devices—surveillance cameras, routers, networked printers, for example—is harnessed as a botnet to communicate with and overwhelm servers and websites. As one threat report notes, this phenomenon is "thriving because organizations and users are deploying low-cost IoT devices rapidly and with little or no regard for security."[47] The most powerful attack in the US to date was on a key internet company (Dyn) that resulted in a sustained interruption of internet service for major companies.[48] Researchers have shown that a manipulation of devices

[41] See Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (March 2015): 75–89, accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

[42] Federal Trade Commission, *Data Brokers: A Call for Accountability and Transparency*, (FTC, May 2014), accessed at https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

[43] Cyware, "Cloud storage data breaches: Why are they so common and what can you do to stay safe?", October 13, 2018, accessed at https://cyware.com/news/cloud-storage-data-breaches-why-are-they-so-common-and-what-can-you-do-to-stay-safe-a17e8975

[44] Swati Khandawal, Medtronics Implantable Defilibrators Vulnerable to Life-Threatening Hacks, Hacker News, March 22, 2019, accessed at https://thehackernews.com/2019/03/hacking-implantable-defibrillators.html and Selena Larson, "FDA Confirms that St. Jude's Cardiac Devices Can be Hacked", *CNN Business*, January 9, 2017, accessed at https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/.

[45]For research on remote hacking of automobiles, see "The Connected Car: Ways to Get Unauthorized Access and Implications", *Computest*, April 2018, accessed at https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/.

[46] [46]Kelly Jackson Higgins, "Researcher Successfully Hacked In-Flight Airplanes - From the Ground", *Dark Reading*, June 6, 2018, accessed at https://www.darkreading.com/threat-intelligence/the-coolest-hacks-of-2018/d/d-id/1333520.

[47] Cisco 2018 Security Report, p 31, accessed at https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2018.html. See also Department of Commerce and Department of Homeland Security*, A Report to the President on Enhancing Resilience of the Internet and Communications Ecosystem against Botnets and Other Automated Distributed Threats*, May 22, 2018, accessed at https://www.commerce.gov/sites/default/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf, p. 5. and pp. 15ff.

[48] Conner Forrest, "Dyn DDoS Attack: 5 Takeaways on What We Know and Why It Matters", *TechRepublic*, October 24, 2016, accessed at https://www.techrepublic.com/article/dyn-ddos-attack-5-takeaways-on-what-we-know-and-why-it-matters/

on the demand side of the power grid—air conditioners, refrigerators, etc.—that are linked as a botnet could create cascading blackouts across regions.[49]

Enhanced risk to critical infrastructure. Many critical infrastructure sectors—the power grid, dams, transportation systems, water treatment facilities, manufacturing plants, for example—rely on industrial control systems (ICS) to remotely manage operations through networks. Based on its engagements, *Dragos*, an ICS security firm, reported that in 2018 only 20%-30% of the entities using ICS in North America have real time monitoring of those systems. In 40% of the cyber incident responses that the firm was involved in, the attacker had been in the network for over a year.[50]

Findings about security vulnerabilities have been published in sector-specific reports. A 2017 consensus report of the National Academies of Sciences, Engineering, and Medicine concluded that the "US grid remains vulnerable to national disasters, physical and *cyber attacks* and other accidental failures".[51] One of its recommendations was to improve "the security and resilience" of cyber monitoring and control systems.[52] Not all vulnerabilities are the result of inherent flaws in software or hardware but pertain to unsound practices.

- In 2017, Duke Power was fined $10 million by the National Electric Reliability Corporation (NERC) for 127 violations of cybersecurity standards that "posed a serious risk to the security and reliability of the BPS (Bulk Power System)" serving millions of customers across seven states.[53] In January of this year, NERC filed a Notice of Penalty with the Federal Electric Regulatory Commission (FERC) stating that certain cybersecurity violations by Duke were ongoing. These included allowing direct "remote access to the BCSs (Bulk Electric System Cyber Systems) inside the Companies ESP (Electronic Security Perimeter) without first going through an Intermediate System, utilizing encryption, and requiring multi-factor authentication."[54]

- A June 2018 Inspector General Report of the Department of the Interior of dams concluded that two dams critical to the nation's security were at risk because of poor computer security practices.[55] These included the failure to limit the number of ICS users with system administrator access and maintaining too many group accounts; not complying with

[49] Andy Greenberg, How Hacked Water Heaters Could Trigger Mass Blackouts, *Wired,* 8/13/18, accessed at https://www.wired.com/story/water-heaters-power-grid-hack-blackout/

[50] Kelly Jackson Higgin, "ICS/SCADA Attackers Up Their Game*", Dark Reading*, February 15, 2019, accessed at https://www.darkreading.com/threat-intelligence/ics-scada-attackers-up-their-game/d/d-id/1333893

[51] Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System, Board on Energy and Environmental Systems, Division on Engineering and Physical Sciences, *Enhancing the Resilience of the Nation's Electricity System*, Washington, DC: National Academic Press (2017), pp. 4 and 135; accessed at https://www.nap.edu/read/24836/chapter/1

[52] Ibid, see for example pp. 119ff

[53] United States of America before the Federal Electric Regulatory Commission, Docket No. NP19-4-000; pp 1-2, accessed at https://michaelmabee.info/wp-content/uploads/2019/02/FERC-Docket-NP19-4-Motion-to-Intervene-Mabee.pdf

[54] Ibid.

[55] Office of the Inspector General, US Department of the Interior, *US Bureau of Reclamation Selected Hydropower Dams at Increased Risk from Insider Threats*, June 7, 2018, pp 5-14, and 27, accessed at https://www.oversight.gov/sites/default/files/oig-reports/FinalEvaluation_ICSDams_Public.pdf

> password policies and removing inactive system administrator accounts; and not following best practices, such as those recommended by the NSA, requiring more rigorous background checks for personnel with elevated system privileges. The report also found that compensating controls such as video surveillance and access card monitoring were reactive, used as investigation tools and not pro-actively to monitor security.

Threats are well documented. US intelligence threat assessments continue to place cyber attacks at the top of the list of national security threats and underscore the risk to critical infrastructure in particular. A recent assessment by the Office of the Director of National Intelligence points to the capacity of nation state actors to disrupt many sectors of critical infrastructure, noting elections, electric distribution, and gas pipelines as examples. Likewise, criminal groups are expected to increasingly target US banking and finance, health care, emergency services, and government operations.[56]

Compromises of critical infrastructure are increasingly high profile. In 2018, DHS and the FBI issued a joint alert that "Russian government cyber actors…gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS)".[57] Top-of-mind, of course, are attempts to hack election systems. Maryland residents are familiar with the reports of the unsuccessful attempt to breach the State's voter registration system and of supply chain concerns triggered by the transfer to a Russian owner of a company providing the platform for the State's voter registration system and other online systems.[58]

State and local governments challenged by the threat environment. The widely reported ransomware attacks on Atlanta last year and on Baltimore this May have focused once again attention on the security posture of state and local governments. Threats are a constant. Between January 2017 and April 2019, there were 112 reported ransomware attacks on these governments in the US.[59] In a 2018 survey of state CISOs, 30 reported security breaches of web applications, 28 discovered malicious code in their systems; 16 noted breaches caused by hackers; and 14 reported physical attacks (e.g., stolen laptops).[60]

[56] Daniel Coates, Director of National Intelligence, *Statement for the Record: Worldwide Threat Assessment of the Intelligence Community*, Senate Select Committee on Intelligence, January 29, 2019, pp. 5-7, accessed at https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community?tmpl=component&print=1

[57] See CISA Alert (TA18-074A) "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", March 15, 2018, accessed at https://www.us-cert.gov/ncas/alerts/TA18-074A.

[58] Jayne Miller, "Maryland voter registration system runs on software owned by Russian-financed firm, I-Team learns", *WBALTV*, July 13, 2018, accessed at https://www.wbaltv.com/article/maryland-voter-registration-system-runs-on-russian-owned-software-i-team-learns/22144023. These concerns were addressed by SB 743 (Election Service Providers – Contract Clauses and Termination of Contracts) which passed in the 2019 session.

[59] Allan Liska, "Early Findings: Review of State and Local Government Ransomware Attacks", *Recorded Future*, April 2019, accessed at https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

[60] See Doug Robinson and Srini Subramanian, Doug Robinson and Srini Subramanian, *2018 Cybersecurity Study, Deloitte-NACIO,* p. 26, accessed at https://documents.deloitte.com/insights/2018DeloitteNASCIOCybersecurityStudy

As a key component of critical infrastructure, the public sector continues to take steps to enhance its security. In the last five years, state governors as a group have issued more than 90 executive orders responding to cyber-related concerns.[61] States have established fusion centers to share threat intelligence across state agencies and with local partners and participate in other intelligence sharing organizations, such as the MS-ISAC. Likewise, states have benefitted from the cyber capabilities of their national guard units and partnerships with the Department of Homeland Security and federal law enforcement agencies.

In its annual assessment, *SecurityScorecard* observes that in 2018 federal, state, and local governments as a group moved up to 11th relative to 20 other industries on overall security measures. In 2017, they ranked third to last.[62] The report noted that particular strengths included "DNS health", lower susceptibility to social engineering attacks, and application security.[63]

State governments on the whole have likewise advanced in the areas of management, governance, and training:

- All 50 states have enterprise CISO roles (established by legislation in 31 states)
- The majority of these CISOs report to senior leaders, either the governor or a cabinet secretary
- 40 states have approved cybersecurity strategy and governance plans
- 47 states have established general cybersecurity-related training programs for state employees[64]

However, for federal, state and local governments in general critical weaknesses continue to exist. *SecurityScorecard* identified endpoint security, network security, and patching cadence as ongoing vulnerabilities. The report notes that "low grades in endpoint security, IP reputation, network security, and patching cadence are highly predictive indicators that an organization may have a higher probability of experiencing an imminent information security incident than an organization with high grades in these areas".[65] Similarly, based on a 2017 survey, the MS-ISAC concluded that state and local governments were below the "minimum maturity level" on almost all five categories of the NIST Cybersecurity Framework (CsF). It forecast that none of these governments will reach "minimum maturity" in all categories until 2023 and 2024, respectively.[66]

The top two challenges state CISOs face are budget and inadequate cybersecurity staffing. As a benchmark, US industry spends an average of 28% of its IT budget on security-related technology. In a 2018 survey, CISOs in 27 states reported that less than 3% of their state's IT

[61] Adam McCormick, research project at the Center for Health and Homeland Security, Francis King Carey School of Law, University of Maryland, March 31, 2019.

[62] SecurityScorecard, 2018 Government Cybersecurity Report, p. 4, accessed at https://explore.securityscorecard.com/rs/797-BFK-857/images/2018%20Government%20Cybersecurity%20Report.pdf

[63] Ibid, pp. 10-12.

[64] Doug Robinson and Srini Subramanian, opus cit, pp. 5, 14-15, 25.

[65] *SecurityScoreCard*, pp. 3, 6-9.

[66] Mutli-State Information and Analysis Center, *2017 Nationwide Cybersecurity Review: Summary Report*, p. 7, accessed at https://www.cisecurity.org/wp-content/uploads/2018/10/NCSR-2017-Final.pdf

enterprise budget (all executive agencies) was spent on enterprise security. Regarding staffing, the average FTE reported by CISOs across all states for their cybersecurity teams was between 6 and 15. Thirty state CISOs reported that their staff have gaps in competencies required to handle cybersecurity requirements. Those qualitative shortcomings are attributed to state pay structures that significantly lag the private sector.[67]

Maryland reflects national trends as discussed under Sections VI and VII below.

Cybersecurity Workforce Shortage. The shortfall in the number of needed professionals continues to be a defining characteristic of the cybersecurity industry. One estimate, informed by NIST's National Cybersecurity Workforce Framework, is that there are well over 300,000 open positions in cybersecurity with the supply of professionals vis-à-vis demand several orders of magnitude below that of other workforce sectors.[68] The need has been described as "urgent" for national security and economic prosperity by both the US DHS and the US Department of Commerce.[69]

As the nation's cyber epicenter, Maryland is affected by this shortage. The State's IT-related tech workforce numbers about 195,000.[70] Currently, there are roughly 46,000 cybersecurity positions in the State with about 15,000 of these unfilled.[71] This shortfall has been persistent despite rising numbers of graduates in cybersecurity and related fields by the State's colleges and universities.[72]

The impact plays out economically. Maryland's gross domestic product in 2018 has been placed at about $418 billion.[73] It is estimated that the direct contribution of the IT-related tech sector to the State's economy was almost 12%.[74] Chronic shortages at the magnitude of 15,000 unfilled positions in just one IT-related sector has cascading impacts on the State's economic growth, tax revenues, and capacity to sustain innovation.

[67] Robinson and Subramanian, opus cit., pp. 6, 9, 19, 21-22.

[68] See Cyberseek at https://www.cyberseek.org/heatmap.html

[69] US Department of Commerce and US Department of Homeland Security, *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future.* November 16, 2017, p. 5, accessed at https://www.dhs.gov/sites/default/files/publications/eo_wf_report_to_potus.pd_.pdf

[70] CompTia, Cyberstates 2019, p 127, accessed at https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2019.pdf

[71] Select Maryland on the heat map at Cyberseek, https://www.cyberseek.org/heatmap.html

[72] For growth in degrees awarded in cybersecurity or related fields by the University System of Maryland (USM), see Cybersecurity Degrees by Degree Level, Field, and Institution, accessed at https://www.usmd.edu/IRIS/DataJournal/CyberSecurity/?report=Degrees-by-Degree-Level-by-Field. See also the 2018 USM case study by the Business Higher Education Foundation: *Building a Diverse Cybersecurity Ecosystem to Address National Security Needs,* accessed at http://www.bhef.com/publications/building-diverse-cybersecurity-talent-ecosystem-address-national-security-needs

[73] Bureau of Economic Statistics News Release 19-04, Table 3 (Current-Dollar Gross Domestic Product [GDP] by State and Region, 2017: Q1 – 2018 Q3), accessed at https://www.bea.gov/system/files/2019-02/qgdpstate0219.pdf

[74] CompTia, opus cit, p. 37.

V. The Council Activities Since July 1, 2017

The foregoing events, findings, and trends have informed the Council's recommendations and the efforts of its members to realize the recommendations' objectives. These efforts have been both legislative and non-legislative.

Legislation sponsored or co-sponsored by the Council's Legislative Members
(Enacted Bills)

2016 Recommendation 4. Facilitating Use of the No-charge Credit Freeze Option
Originating Council Subcommittee: Law, Policy and Legislation

In the 2018 session, Council members Senator Lee and Delegates Carey and Lisanti successfully sponsored SB 202/HB 710 (Consumer Protection - Credit Report Security Freezes - Notice and Fees).[75] Co-sponsors included Senators Ferguson, Guzzone, Kelley, King, Pinsky, Rosapepe, Smith, and Zucker, Middleton, Astle, Benson, Feldman, Hershey, Jennings, Klausmeier, Mathias, and Reilly.

The Act became effective October 1, 2018. It relieves consumers, including protected consumers, of any fees involved in managing access to their credit reports after being affected by a breach. Specifically, it prohibits credit reporting agencies from charging a fee of an affected consumer for the *placement, removal, or temporary lift* of a security freeze. The Act built on SB 270/HB 212 (sponsored by Senator Lee and Delegate Carey) that passed the 2017 session and prohibited fees for consumers initiating a credit freeze after notification of being affected by a breach. The purpose of the Council's recommendation and both laws is to encourage consumers to be proactive in protecting their identities when notified of a breach involving their personal identifying information.

2017 Recommendation 9. Implementation of a comprehensive Computer Network Defense Program to provide robust protection to State assets, business information, and citizen data across all agencies.
Originating Subcommittee: Cyber Operations and Incident Response

SB 553 (State Government - Security Training - Protection of Security-Sensitive Data).[76] As an incremental step, this furthers the Council's 2017 recommendation 9. Sponsored by Senator Simonaire, the statute requires that all units of State government develop a plan and execute training for employees handling "security sensitive" information held on organizations and private citizens. DoIT had been offering such training to agencies. But this bill, which became law on June 1, 2018, and included certain reporting requirements, made it mandatory that all State agencies participate in the training.

[75] See p. 1 for citation.
[76] Ibid.

2016 Recommendation 11. Maryland Scholarship for Service Program.
Originating Council Subcommittee: Education and Workforce Development

Sponsored by Senator Simonaire and Senator Lee, SB 204 (Cybersecurity Public Service Scholarship Program) passed in the 2018 session.[77] The bill's objective was to address in some measure the Council's concern about the cybersecurity workforce shortage affecting State government and the cybersecurity teacher shortage in Maryland public schools. It became effective July 1, 2018.

The law establishes a cybersecurity scholarship-for-service program very similar to the federal program administered by the National Science Foundation. Under SB 204, full-time undergraduate and graduate students in degree programs directly relevant to cybersecurity at qualifying institutions are eligible for scholarships. In return for each year of scholarship support, program graduates must complete a one-year obligation within a unit of State government in a cybersecurity work role or teach in a public high school in a curriculum directly related to cybersecurity. In its first year, 190 applications for the scholarship were received. The program was funded at $160,000 in FY 2019 and will remain at that level in FY 2020.

Legislation sponsored or co-sponsored by the Council's Legislative Members
(Bills Proposed But *Not* Enacted)

Members of the Council's legislative delegation sponsored or cosponsored bills which, while not enacted in 2018 or 2019, nonetheless attempted to realize the recommendations of the Council in some form. These efforts include the following:

2016 Recommendation 2. Updates to the Maryland Personal Information Protection Act
Originating Council Subcommittee: Law, Policy, and Legislation

SB 786/HB 1127 (Financial Consumer Protection Act) was a wide-ranging bill sponsored by Senator Rosapepe that generally implemented the recommendations of the Maryland Financial Consumer Protection Commission. Of particular interest to the Council, were proposed amendments to Sections 14-3501, 14-3503, 14-3504 of the Commercial Article which would have updated the Maryland Personal Information Protection Act in a number of ways. The bill was co-sponsored by Senator Lee and by Delegate Carey on the Council who were joined by Senator Ferguson and Senator Washington and Delegate Hill.

As proposed, SB 786/HB 1127 would have expanded the definition of personal information to include activity tracking data and genetic information, reduced the notification period to consumers from the current 45 days to 10 days (starting from the point of discovery but permitting organizations more time before notification as is practically necessary to determine

[77] Ibid.

the facts around the breach), required direct notification of consumers in all breach cases, among other changes. The bill received an unfavorable report by the Senate Finance Committee.

2017 Recommendation 2. Legislative 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.
Originating Council Subcommittee: Law, Policy, and Legislation

In the 2018 session, Senator Lee sponsored SB 882 (Procurement - Telecommunication and Computer Network Access - Security Requirements). Relative to the recommendation, the bill would have required vendors of internet-connected devices to the State to either a) warrant that those devices are free of certain specified vulnerabilities or b) have the requirement waivered by going through a review process. The Department of Information Technology would have been required to develop procedures to implement the bill. In making the recommendation underlying the bill, the Council was sensitive to the 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.

2017 Recommendation 4. Inclusion of a ransomware definition in Maryland's extortion statute or a new code section with increased penalties for extortion levels below the general extortion statute threshold.
Originating Council Subcommittee: Law, Policy, and Legislation

Versions of a ransomware bill were proposed in the 2018 and 2019 sessions. In the 2018 session, Council members Senator Lee and Senator Simonaire proposed SB 376/HB 456 (Criminal Law - Crimes Involving Computers - Cyber Intrusion and Ransomware). In the 2019 session, both Senators proposed SB 151 (Criminal Law – Crimes Against Computers – Ransomware) which was cross-filed as HB 211 by Delegates Barron and Fisher.

In the main, SB 151/HB 211 was very similar to a statute enacted in Michigan in 2018.[78] SB 151/HB 211 made the knowing possession of ransomware with intent to use for specified purposes a violation of the criminal law, provided a research exception, and permitted the right of private action for those directly injured by a ransomware attack. Despite attention in the Baltimore media and broader support in the Senate, the bill was not brought to a vote in the Senate Judicial Proceedings Committee or the House Judiciary Committee. Other Senators supporting the bill included Beidle, Carter, Elfreth, Griffith, Guzzone, Kagan, King, Kramer, Lam, Patterson, Rosapepe, Smith, Waldstreicher, Washington, West, and Young.

[78] See Michigan 2018 HB 5257 at https://www.legislature.mi.gov/documents/2017-2018/publicact/htm/2018-PA-0095.htm

2017 Council Recommendation 6. Legislation that would require IoT devices to include consumer labelling about the security features the devices incorporate.
Originating Council Subcommittee: Law, Policy, and Legislation

Senator Lee and Delegate Carey introduced SB 553/HB 1276 (Security Features for Connected Devices) in the 2019 session. It was co-sponsored by Senators Elfreth, Guzzone, Nathan-Pulliam, Smith, Waldstreicher, Washington, and Young.

The Council's recommendation, like the bill itself, was motivated by the concern about the abuses to which insecure devices expose consumers and the wider society. As discussed in Section IV, these abuses range from strangers intercepting the feeds of baby monitors to the exploitation of these devices for devastating denial-of-service attacks that cripple websites and even the ability of the internet itself to function.

As a first attempt to improve the security of these devices, the bill would have required that manufacturers of such devices sold in Maryland to ensure that the passwords either be unique to each device (if hardwired) or require the consumer to change the password before the device authenticates to the internet. The bill was not brought to a vote by either the Senate Finance Committee or the House Economic Matters Committee.

2017 Council Recommendation 7. 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.
Originating Council Subcommittee: Law, Policy, and Legislation

In the 2019 session, Senator Lee and Delegate Carey proposed SB 613/HB 901 (Online Consumer Protection Act). Delegates Brooks and Hill co-sponsored the House bill. Modelled on the California Consumer Protection Act which will take effect in 2020, SB 613/HB 901 would have enabled Maryland consumers to know the vast amount of personal information that social media platforms and other commercial entities compile on them from multiple sources, to delete information, and to prohibit the sale of their personal information in whole or in part to third parties. It would have prohibited the sale to third parties of personal information collected of known minors. The bill was not brought to a vote by either the Senate Finance Committee or the House Economic Matters Committee.

Non-legislative Council Activity

Recommendation 17: Cybersecurity Repository
Originating Council Subcommittees: Subcommittee on Critical Infrastructure and Subcommittee on Public and Community Outreach

In early 2018, the Council launched a searchable repository of curated cybersecurity guidebooks, reports and other resources. The repository is focused on critical infrastructure owners and operators as well as small- and medium-size businesses, and consumers, concentrating resources that are likely to be most appropriate for these stakeholders. Since its launch the repository has collected about 200 resources. The collection is managed for the Council through a partnership between the Center for Health and Homeland Security at the Francis King Carey School of Law and the University of Maryland Global Campus. The repository can be accessed at http://www.umuc.edu/mdcybersecuritycouncil.

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.
Originating Council Subcommittee: Cyber Operations and Incident Response

With a view to the State government's cybersecurity, the Council scheduled a number of briefings in late 2017 and early 2018 on the needs of DoIT to implement a mature cybersecurity program across State agencies. This information was incorporated into an analysis of the Council's Subcommittee on Cyber Operations and Incident Response and was later included in the July 2017 Activities Report. The objective was to try to quantify the fiscal effort that would be required of the State for DoIT to implement Recommendation 9. As an outcome, the Council endorsed a resolution at its October 25, 2017, meeting urging an investment of $28.9 million dollar in DoIT's cybersecurity function with an annual, inflation-adjusted sustainment budget of $14 million to $15 million dollars thereafter.

Other Non-legislative Activities

As an ongoing outreach initiative, the Council continues to organize an annual reception in Annapolis at the beginning of session with subject matter experts to discuss cybersecurity issues for legislators and their staff. The Council's January 2018 reception included Deborah Plunkett, former director of the NSA's Information Assurance Directorate and a Senior Fellow at Harvard University's Belfer Center for Science and Technology. The 2019 speaker was Lt. General Harry Raduege Jr. (USAF, Ret), former Director of the Defense Information Systems Agency (DISA) within the US Department of Defense.

Not responsive to a recommendation of record but recognizing the present ransomware emergency in Baltimore City, the Council approved a resolution at its May 22, 2019, meeting encouraging any members to volunteer their expertise to the special security committee convened by Baltimore Council President Brandon Scott. Five Council members, all faculty of Baltimore-area schools, responded to the call and were subsequently identified to Mr. Scott in a letter representing the Council. As the staffing agency for the Council, University of Maryland Global Campus also notified the City of two of its faculty willing to volunteer their time and expertise.

VI. Other Noteworthy Developments Related to the Council's Recommendations

This report strongly commends the efforts of others, acting independently and according to their own policy agendas, in ways that realize the objectives of Council recommendations.

2017 Recommendation 9. Implementation of a comprehensive Computer Network Defense Program to provide robust protection to State assets, business information, and citizen data across all agencies.
Originating Subcommittee: Cyber Operations and Incident Response

The Governor's October 2017 and June 2019 executive orders have launched important efforts to enhance the cybersecurity posture of State Executive Branch and to protect the confidentiality, integrity, and availability of its systems and the sensitive data they hold.[79]

The 2017 Executive Order (Maryland Cybersecurity) convened a working group of cybersecurity stakeholders from across State agencies to confirm certain baseline information related to cybersecurity within the executive branch and to make recommendations based on those findings. In consequence, DoIT is pursuing a number of specific goals that it hopes to implement in tandem with a deeper assessment of the security posture and practices of agencies. These goals include:

- Consolidating security tools across State agencies in order to reduce cost and improve efficiency
- Standardizing governance processes, structures and documentation so as enhance the State's ability to respond to an incident since agencies will be operating from a common framework
- Institutionalizing pen testing and red/blue exercises to support a proactive security posture
- Continuing to build stakeholder collaboration across State agencies
- Implementing modern data privacy practices ala HB 716 (State Government - Protection of Information - Revisions (Maryland Data Privacy Act) that narrowly failed in the 2019 session[80]
- Seeking breach notification requirements for all three branches of State government and local jurisdictions on the grounds that reporting produces greater awareness of the threat landscape—who has been compromised and how—contributing to collective security.

To help ensure that the executive branch pursues unified cybersecurity strategy, policy and practice and that it is better positioned to manage the consequences of cybersecurity incidents, the June 2019 Executive Order (Maryland Cyber Defense Initiative) makes a number of crucial organizational changes.[81] Specifically, it:

[79] See note, p. 3, for reference.
[80] The bill can be found at http://mgaleg.maryland.gov/2019RS/fnotes/bil_0006/hb0716.pdf
[81] See Sections B, C and D.

- Clearly elevates the DoIT CISO to an executive branch-wide role. This is indicated by the name, "State Chief Security Officer" (SCISO), and the manner of appointment (by the Governor). The SCISO will continue to report to and be supervised by the DoIT Secretary.
- Renames the former DoIT CISO's office as the "Office of Security Management", centralizing within it the direction, coordination, and implementation of the overall cybersecurity strategy and policy for the Executive Branch of State government
- Creates a stakeholder group of State officials or their designees (the "Maryland Cybersecurity Coordinating Council") to advise the SCISO on "the strategy and implementation of cybersecurity initiatives and recommendations" and on "building and sustaining the State's capability to identify, mitigate, and detect cybersecurity risk, and respond to and recover from cybersecurity- related incidents". This Coordinating Council includes the Adjutant General of the State's National Guard, which has well-developed cybersecurity capabilities that can be activated to support State entities.[82]

The Council's 2016 Recommendation 10. Basic Computer Science and Cybersecurity Education in Maryland
Originating Council Subcommittee: Education and Workforce Development

The 2018 session passed HB 281(Computer Science - Curriculum and Professional Development [Securing the Future: Computer Science Education for All].[83] The bill reflected a concern, expressed in a number of venues, that computer science education should be mandated in Maryland K12 education. The bill was proposed by Delegate Miller and co-sponsored by Delegates Dumais, Fennell, Fraser–Hidalgo, Gibson, Hill, Jalisi, Korman, Krimm, Lam, J. Lewis, Lierman, McCray, McIntosh, Moon, Rose, Rosenberg, Saab, Sample–Hughes, Sophocleus, Tarlau, Valderrama, and M. Washington. The Act took effect on June 1, 2018.

The law stipulates that beginning in 2021-2022 each county school board must require each public high school to offer at least one computer science course of high quality and must make efforts to incorporate computer science in elementary and middle schools and to increase the number of under-represented groups in computer science. It additionally establishes the Maryland Center for Computing Education at the University System of Maryland to expand access to computer science K12 education, offer professional development for computer science teachers, and increase the number of K12 computer science teachers. The Act called for $300,000 start-up funding in FY 2019 and at least $1,000,000 funding in each of FY 2020 and FY 2021.

The Council's 2016 Recommendation 16: Cybersecurity Business Accelerators
Originating Council Subcommittee: Economic Development

[82] State entities are supported by the National Guard primarily through the Maryland Emergency Management Agency. The Maryland National Guard has two major cyber defensive units: the 169th Cyber Protection Team within the Army Guard and the 275th Cyber Operations Squadron (also a Cyber Protection Team) within the Air National Guard.

[83] See p. 3 for citation.

In 2018, Senator Guzzone proposed SB 228 (Cybersecurity Incentive Tax Credits) which became effective on June 1, 2018.[84] Senate co-sponsors included Eckardt, Edwards, and Serafini. The bill ultimately included provisions of SB 310/HB 364(Cybersecurity Act of Maryland). The Act extends the cybersecurity investment tax credit through 2023 while changing the tax credit from the cybersecurity firm to the investor. The Act also includes a "buy Maryland" credit against the State income tax for qualifying firms purchasing cybersecurity services or technology from Maryland vendors meeting certain requirements. The amount of the credit is 50% of the qualified cost, not to exceed $50,000 for each qualified buyer.

The bill was consistent with proposals of the Council's Subcommittee on Economic Development to make the investment tax credit work better as an investment incentive and to encourage Maryland firms to purchase Maryland cybersecurity products and services.

VII. The Next Two Years

The Council reaffirms its recommendations to date that either have not been realized or are of a nature requiring ongoing attention. In upcoming sessions, the Council and its members will give particular attention to:

- 2016 Recommendation 2. Updates to the Maryland Personal Information Protection Act
- 2016 Recommendation 8. Educational resources for small- and medium-size organizations--particularly critical infrastructure owners—and consumers.
- 2016 Recommendation 12. Resources for public university computer science departments as a strategic State investment in workforce development and innovation.
- 2017 Recommendation 4. Inclusion of a ransomware definition in Maryland's extortion statute or a new code section to address the ransomware threat.
- 2017 Recommendation 6. Measures addressing the insecurity of Internet of Things (IoT) devices.
- 2017 Recommendation 7. Legislation to ensure the transparency of consumer information held by data brokers and other entities, the right of consumers to inspect and correct wrong data, and their right to opt out of the sale of data to third parties.
- 2017 Recommendation 9. 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. Clearly, the 2017 and 2019 Executive Orders have driven significant changes that will enhance the cybersecurity posture of the State's Executive Branch. To be commended too is the increase in funding for new initiatives of the Office of Security Management. Nonetheless, the Council believes that investments at the much higher levels it recommended must follow by one means or another to fully realize the promise of these important Executive Orders.[85]

In addition, the Council affirms several new recommendations proposed by the following subcommittees for its attention in FY 2020 and 2021:

[84] Ibid.

[85] See pp 3-4 and 22.

Joint recommendation of the Subcommittee on Law, Policy and Legislation and the Subcommittee on Critical Infrastructure

2019 Recommendation 1. The State should prioritize assessing the security vulnerabilities of its absentee balloting system. Available to all voters, and instrumental in expanding the franchise to disabled voters and to UOCAVA and non-UOCAVA voters abroad, Maryland's absentee balloting system is nonetheless potentially susceptible to manipulation. [86] A bill to limit the use of certain of the means for voters to receive absentee ballots failed in the last legislative session.[87] The State Board of Elections should be directed to devote new federal grant money to assessing the security vulnerabilities of its absentee balloting system and to put in place a program of mitigation where needed.

Subcommittee on Law, Policy and Legislation

2019 Recommendation 2. North Dakota Senate Bill 2110 should be considered in conjunction with all interested stakeholders to understand to what extent it could serve as a model for Maryland by enlarging DoIT's role with respect to the other branches of State government as well as local governments and the public university system.[88]

Subcommittee on Critical Infrastructure

2019 Recommendation 3. The State should act to support the cybersecurity of the electric utilities serving Maryland. Noted in this connection are actions taken by California, Michigan and other states in consultation with their utility stakeholders.[89]

Joint Recommendation of the Subcommittee on Critical Infrastructure and Subcommittee on Economic Development

2019 Recommendation 4. Information Sharing and Analysis Organization (ISAO). The State should establish or facilitate an information sharing and analysis organization especially targeted at small and medium-size businesses in Maryland. Such an organization would enable small and medium-size business to better protect themselves against breaches by receiving timely threat information, breach mitigation assistance, advice on steps to take to protect themselves, and

[86] See for example Jodie Fleischer, Katie Leslie, Jeff Piper, Steve Jones and Chester Panzer, "In Wake of Russian Meddling, Critics Say Maryland's Online Ballot System Is Potential Target", October 20, 2018, *NBC News4*, accessed at https://www.nbcwashington.com/investigations/In-Wake-of-Russian-Meddling-Critics-Say-Marylands-Online-Ballot-System-Is-Potential-Target-497948281.html and more recently, Jodie Fleischer, Katie Leslie, Steve Jones and Chester Panzer, "Maryland Legislators Consider Limiting Electronic Absentee Ballots", NBC News4, February 27, 2019, accessed at https://www.nbcwashington.com/investigations/Maryland-Legislators-Consider-Limiting-Electronic-Absentee-Ballots-506449371.html

[87] See HB 706 (Election Law - Absentee Ballot Requests, Delivery, and Marking). The bill and the fiscal policy note can be accessed at http://mgaleg.maryland.gov/webmga/frmMain.aspx?id=hb0706&stab=01&pid=billpage&tab=subject3&ys=2019RS

[88] See SB 2110 at https://www.legis.nd.gov/assembly/66-2019/documents/19-8091-04000.pdf

[89] See Adam McGovern, Justin Somelofske, Claire Valentine-Fossum, Kristen Zweifel, and Mark James, *Improving the Electric Grid*, The Institute for Energy and the Environment, University of Vermont Law School, April 2019, accessed at https://www.vermontlaw.edu/sites/default/files/2019-04/VLS_IEE_Electricity_Distribution_Grid_Cybersecurity_Phase_1%20Report%5B1%5D.pdf

proactive training. There are different models that State policymakers can consult for this purpose.[90]

Subcommittee on Economic Development

2019 Recommendation 5. Cybersecurity Workforce Development. The State should consider the following: a) raising the cap for employer reimbursement of wages paid to technical interns and apprentices in cybersecurity to a level approaching a greater percentage of the actual wage paid, and b) a scholarship forgiveness program for cybersecurity graduates that remain in state for some stipulated number of years. The latter would mirror the program currently offered to life science graduates.

Recommendation 6. Support for IP Start-ups. Institution of an R/D tax credit against employer-paid State and local taxes and filing fees for qualifying cybersecurity product start-ups.

Recommendation 7. Implementing a tax credit analysis in coordination with the Maryland Department of Commerce to review existing tax credits to do the following: consolidate existing tax credits, eliminate redundant or obsolete credits, and streamline the application and award process for receive available tax credits. Mindful of the competing demands on the State, but with an eye to supporting growth in the State's business base, the Council further recommends that so much as possible relevant existing tax credits be extended to provide longer availability and available funds for existing tax credits be increased.

VIII. Conclusion

The Maryland Cybersecurity Council performs an important role within Maryland's cybersecurity ecosystem. Comprised of representatives from across private critical infrastructure sectors, government, higher education, and advocacy groups, among others, the Council offers expertise to help inform the cybersecurity policy deliberations of the State's executive and legislative branches. This partnership makes Maryland stronger.

The 2017 Executive Order (Maryland Cybersecurity) directed that the Council's recommendations should be consulted as appropriate by the working group convened under the order. Similarly, SB 339 (Public Safety 9-1-1 Emergency Telephone System) passed in 2019 mandates that cybersecurity standards for public service answering points be developed in consultation with the Council. Finally, as noted, within the last two years the objectives of three of the Council's own recommendations have been effectuated in whole or in part in law. The Council looks forward to continuing to contribute to the State's cybersecurity policy.

[90] See the Arizona Threat Response Alliance at https://azinfragard.org/actra/ or the New Jersey Cybersecurity and Communications Integration Cell at https://www.cyber.nj.gov/

IX. More Information

Questions may be addressed to:

University of Maryland Global Campus
ATTN Maryland Cybersecurity Council Staff
3501 University Boulevard East
Adelphi, Maryland 20783
Marylandcybersecuritycouncil@umuc.edu[91]

[91] This report was drafted by Dr. Gregory von Lehmen, Special Assistant to the President for Cybersecurity, University of Maryland Global Campus, and Staff to the Maryland Cybersecurity Council. It was reviewed by the Council and approved by the Office of the Attorney General.

APPENDIX A

Consolidated 2016 & 2017 Recommendations of the Maryland Cybersecurity Council

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

2017 Recommendations		Originating Subcommittee
1.	Update the State's Executive Branch breach law and extend personal information privacy protections and breach reporting requirements to the judicial and legislative branches.	Law, Policy, and Legislation
2.	Legislative 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.	
3.	Legislation requiring express consumer consent for internet service providers (ISPs) to sell or transfer consumer internet browser history.	

	2017 Recommendations (Continued)	**Originating Subcommittee**
4.	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.	Law, Policy, and Legislation
5.	Legislation to create 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.	
6.	Legislation that would require IoT devices to include consumer labelling about the security features the devices incorporate	
7.	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.	
8.	Maryland develop capability for sharing cybersecurity information and providing outreach support.	Critical Infrastructure Subcommittee & Incident Response and Cyber Operations Subcommittees (Joint Recommendation)
9.	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	Cyber Operations and Incident Response Subcommittee

APPENDIX B

Maryland Cybersecurity Council Members by Sector

Chair

Attorney General Brian Frosh

Legislative Representatives

Senator Susan C. Lee (District 16)
Senator Bryan W. Simonaire (District 31)
Delegate Ned Carey (District 31A)
Delegate MaryAnn Lisanti (District 34A)

State Institutions

David Engel
Director
Maryland Coordination and Analysis Center

Fred Hoover, Esq.
Assistant People's Counsel
Maryland Office of the People's Counsel

Cal Bowman, designee for Walter F. "Pete" Landon
Director
Governor's Office of Homeland Security

Linda Lamone
Administrator of Elections
State Board of Elections

Michael Leahy
Secretary of Information Technology
Department of Information Technology

Col. William Pallozzi
Secretary of State Police
Department of State Police

Ken McCreedy, designee for Kelly M. Schulz
Secretary
Maryland Department of Commerce

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

Russell Strickland
Director
Maryland Emergency Management Agency

Cybersecurity Companies

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

James Foster
CEO
ZeroFox

Zuly Gonzalez
Co-Founder and CEO
Lightpoint Security

Terri Jo Hayes
Cybersecurity Strategist
mfusion

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

Miheer Khona
CEO
Rising Sun Advisors

Larry Letow
President
LG-Tech

Rajan Natarajan
CEO
QualityPro, Inc.

Jonathan Powell
Senior Director, Software Engineering
General Dynamics Information Technology

Jonathan Prutow
Information Assurance Policy SME
Invictus International Consulting

Business Associations

Brian Corbett, designee for George Davis
Executive Director
TEDCO

Anthony Lisuzzo, designee for Tom Albro
President
Army Alliance

Don Fry
President and CEO
Greater Baltimore Committee

Brian Israel
Business Development Executive
Maryland Association of Certified Public Accountants

Mathew Lee
CEO
Fastech

Marty Rosendale
CEO
Maryland Tech Council

Joe Morales, Esq.
Attorney
Maryland Hispanic Chamber of Commerce

Christine Ross
CEO
Maryland Chamber of Commerce

Stacey Smith
Executive Director
Cybersecurity Association of Maryland

Steve Tiller, designee for Doreen E. Harwood
President
Fort Meade Alliance

Higher Education

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

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

Cyril Draffin
Project Advisor
MIT Energy Initiative

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

Jonathan Katz, PhD
Professor, and Director, MC2
University of Maryland, College Park

Patrick Feehan
Information Security Director, Privacy Director, and Data Protection Officer
Montgomery College

Marcus Rauschecker, JD
Cybersecurity Program Director
Center for Health and Homeland Security
University of Maryland Francis King Carey School of Law

Dr. Kevin Kornegay, designee for David Wilson, EdD
President
Morgan State University

Crime Victim Representative

Sue Rogan
Director of Financial Education
Maryland CASH Campaign

Susceptible Industries

Kristin Jones Bryce
Senior 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

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

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

Other Designees

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

Other Designees (Continued)

Robert W. Day Sr.
Councilman
College Park City Council

Howard Feldman, Esq.
Partner
Whiteford Taylor Preston

Blair Levin
Nonresident Senior Fellow, Metropolitan Policy Program
Brookings Institution

Paul Tiao, Esq.
Partner
Hunton & Williams, LLP

APPENDIX C

Maryland Cybersecurity Council Repository

Resources Added in 2018

Subcommittee on Critical Infrastructure

	Format	URL	Resource Type	Sector	Topic	Author	Organization	Keywords	Skill
	PDF		General Resource	CI sector	Information Assurance	Academic Institution	NIST	Add if listed in the resource.	Beginner
	Video		Guide	Education	Internet of Things	Corporation	FBI	Otherwise UMUC will identify.	Intermediate
	Website		Report	Individual Consumers	Preparedness	Government	DOJ		Advanced
			Tool		Privacy	International Organization	FCC		
					Risk Assessment	Nonprofit	etc.		
					Risk Management				
					Security Breaches				
					Standards				
					Vulnerabilities				
Intragency Report on Status of International Cybersecurity Standardization for the IoT	PDF	https://csrc.nist.gov/publications/detail/nistir/8200/draft	Report	CI sector	Internet of Things	Government	NIST	Cybersecurity, cybersecurity risks, IoT	Advanced
Testimony Threats to Small Business	PDF	https://www.justice.gov/sites/default/files/testimonies/witnesses/attachments/2018/05/01/01-30-2018_howard_s._marshall_fbi_small_business_information_sharing_combatting_foreign_cyber_threats.pdf	General Resource	CI Sector	Risk Management, Vulnerabilities	Government	FBI	Cybersecurity, private sector, small business	Beginner
UK Active Defense Yr. 1	PDF	https://www.ncsc.gov.uk/information/active-cyber-defence-one-year	General Resource	Education	Risk Management	Government	UK National Cyber Security Center	Cybersecurity	Advanced
2018 Hiscox Cyber Readiness Report		https://www.hiscox.com/sites/default/files/content/2018-Hiscox-Cyber-Readiness-Report.pdf	Report	CI sector	Preparedness	International Organization	Hiscox	Cybersecurity, Preparedness	Intermediate
FERC Proposed Supply Chain Reliability	PDF	https://www.ferc.gov/whats-new/comm-meet/2018/011818/E-2.pdf	General Resource	CI sector	Standards	Government	FERC	Supply Chain, Risk Management, Standards	Advanced

Threat, Monitoring, Detection, Response	PDF	https://cdn2.hubspot.net/hubfs/472699/White_Paper/2017-Threat-Monitoring-Detection-Response-Report-2.2.pdf?__hssc=103559903.1.1505832642816&__hstc=103559903.6089a0b883f9683b841b9085cabd5983.1505832642815.1505832642815.1505832642815.1&__hsfp=2820409192&hsCtaTracking=a3914258-2428-4210-ae2f-37da6d469262%7C0f0188ab-f62e-4e12-a4dd-74acfa2ba7a9	Report	CI sector	Risk Assessment	Nonprofit	Information Security	Threat, Confidence	Intermediate
Artificial Intelligence, Big Data and Cloud Taxonomy	PDF	https://en.calameo.com/books/0000097792ddb787a9198	Report	CI sector	Internet of Things	Government	Department of Defense		Intermediate
A report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats	PDF	https://csrc.nist.gov/publications/detail/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final	Report	CI sector	Risk Management	Government	The Secretary of Commerce and the secretary of Homeland Security	Internet Ecosystem	Intermediate
Spectre Attacks: Exploiting Speculative Execution	PDF	https://spectreattack.com/spectre.pdf	General Resource	Education	Risk Management	Academic Institution	University of Pennsylvania and University of Maryland		Advanced
Take Back Control of Your Cybersecurity Now	PDF	https://cdn2.hubspot.net/hubfs/2558521/take-back-control-of-cybersecurity-2017-01.pdf?t=1484087545745	General Resource	CI sector	Risk Management		Advisen		Beginner
Foundational Services and Capabilities	PDF	https://www.isao.org/products/isao-200-1-foundational-services-and-capabilities/	Tool	GI Sector	Privacy, Information Assurance	International Organization	ISAO SO		Advanced

Aviation Cybersecurity, Finding Lift, Minimizing Drag	PDF	http://www.atlanticcouncil.org/publications/reports/aviation-cybersecurity-finding-lift-minimizing-drag	Report	GI Sector	Risk Management	International Organization	Atlantic Council		Beginner
CISO Tips: Balancing the Hero with the Storyteller	PDF	https://www.cybereason.com/blog/blog-ciso-tips-balancing-the-hero-with-the-storyteller	General Resource	GI Sector	Risk Management	Company	Cybereason		Beginner
Grid Security Exercise	PDF	https://www.nerc.com/pa/CI/CIPOutreach/GridEX/NERC%20GridEx%20III%20Report.pdf	Report	GI Sector	Preparedness	Company	NERC		Advanced
Prepared Testimony of Richard F. Smith	PDF	https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf	General Resource	GI Sector	Security Breaches		Richard F. Smith		Beginner
DNS Risk Assessment	PDF	https://www.us-cert.gov/sites/default/files/c3vp/DNS_Risk_Assessment.pdf	General Resource	GI Sector	Risk Assessment	Government	Homeland Security		Advanced
Advancing the Homeland Security Information Sharing Environment: A Review of the National Network of Fusion Centers	PDF	https://www.hsdl.org/?abstract&did=805450	General Resource	GI Sector	Information Assurance	Organization	House Homeland Security Committee		Intermediate
GAO Cyber Work Force	PDF	https://www.gao.gov/products/GAO-18-175	General Resource	GI Sector	Preparedness	Organization	GAO		Intermediate
The Millennial Generation	PDF	https://www.brookings.edu/research/millennials/	General Resource	GI Sector	Preparedness	Organization	Brookings Metropolitan Policy Program		Beginner
The National Security Innovation Base	Video	https://www.newamerica.org/international-security/events/innovation-base/	General Resource	GI Sector	Preparedness	Company	Govini		Beginner
SEC Guidance on Incident Disclosure	PDF	https://www.sec.gov/rules/interp/2018/33-10459.pdf	Guide	GI Sector	Privacy	Government	Securities and Exchange Commission		Beginner

Ten Cybersecurity Tips For Small Businesses	PDF	http://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db1018/DOC-306595A1.pdf	General Resource	CI Sector	Preparedness	Government	Federal Communications Commission		Beginner
Cyberplanner for Small Businesses	Website	https://www.fcc.gov/cyberplanner	Guide	CI Sector	Risk Assessment	Government	Federal Communications Commission		Intermediate
National Cybersecurity Awareness: Small Businesses	PDF	https://www.dhs.gov/sites/default/files/publications/Small%20Business%20Presentation.pdf	General Resource	CI Sector	Preparedness, Vulnerabilities	Government	Department of Homeland Security		Beginner
Entrepreneurs Tip Card	PDF	https://www.dhs.gov/sites/default/files/publications/Entrepreneurs%20Tip%20Card.pdf	Guide	CI Sector	Preparedness	Government	Department of Homeland Security		Beginner
Cybersecurity Planning Guide	PDF	https://www.dhs.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide.pdf	Guide	CI Sector	Preparedness	Government	Federal Communications Commission		Beginner
Mobile Security Tip Card	PDF	https://www.dhs.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_7.pdf	Guide	CI Sector	Preparedness	Government	Department of Homeland Security		Beginner
Cybersecurity Tips for Bloggers	PDF	https://www.dhs.gov/sites/default/files/publications/Social%20Media%20Guide_7.pdf	Guide	CI Sector	Preparedness	Government	Department of Homeland Security		Beginner
Internet of Things Tip Card	PDF	https://www.dhs.gov/sites/default/files/publications/Internet%20of%20Things%20Tip%20Card_7.pdf	Guide	CI Sector	Preparedness	Government	Department of Homeland Security		Beginner
Small Business Information Security: The Fundamentals	PDf	https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf	Gen+I62eral Resource	CI Sector	Preparedness, Risk Management	Government	National Institute of Standards and Technology		Intermediate
10 Cybersecurity Mistakes Your Small Business Cannot Afford to Make	Video	https://www.youtube.com/watch?v=KLrnI5ZEI9Y&feature=youtu.be	General Resource	CI Sector	Preparedness	Government	Small Business Administration		Beginner

Cybersecurity for Small Businesses Course	Video (Flash)	https://www.sba.gov/course/cybersecurity-small-businesses/	General Resource	CI Sector	Preparedness	Government	Small Business Administration		Beginner
Cyber Information Sharing and Collaboration Program	PDF	https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf	Guide	CI Sector	Risk Management	Government	Department of Homeland Security		Intermediate
You've Been Breached, Now What?	Website	https://www.scmagazine.com/home/news/youve-been-breached-now-what/	Guide	CI Sector	Security Breaches	Corporation	SC Magazine		Beginner
Data Breach Response Guide	PDF	http://www.experian.com/assets/data-breach/white-papers/experian-2017-2018-data-breach-response-guide.pdf	Guide	CI Sector	Security Breaches	Corporation	Experian		Intermediate
Data Breach Response: A Guide for Business	PDF	https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf	Guide	CI Sector	Security Breaches	Government	Federal Trade Commission		Beginner
Guide to Developing a Data Breach Response Plan	PDF	https://www.oaic.gov.au/resources/privacy-law/privacy-archive/privacy-resources-archive/guide-to-developing-a-data-breach-response-plan.pdf	Guide	CI Sector	Security Breaches	International Government	Office of the Australian Information Commissioner		Beginner
Data Breach Prevention and Response Guide for Small Businesses	PDF	https://www.ohioattorneygeneral.gov/Files/Publications-Files/Publications-for-Business/Data-Breach-Prevention-and-Response-Guide-for-Smal.aspx	Guide	CI Sector	Security Breaches	Government	Ohio Attorney General		Beginner
To Do Business With Europe, Protect Personal Data	PDF	https://www.dorsey.com/~/media/files/uploads/images/cattanach_gdpr.pdf?la=en	Guide	CI Sector	Standards	Government	Department of Commerce		Intermediate

Tips for U.S. Companies in the Age of EU GDPR and Privacy Shield	PDF	https://www.bna.com/uploadedFiles/BNA_V2/Legal/Pages/Custom_Trials/BLPV/Tips_for_US_Companies_EU_GDPR_Privacy_Shield_final.pdf	General Resource	CI Sector	Preparedness	Corporation	Bloomberg Law		Advanced
Seven Steps for Businesses to Get Ready for the General Data Protection Regulation	PDF	https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-business-7-steps_en.pdf	Guide	CI Sector	Preparedness	International Government	European Union		Beginner
Statement on the Internet of Things and Cybersecurity	PDF	https://www.uschamber.com/sites/default/files/statement_on_the_iot_and_cybersecurity_final_june_2017.pdf	General Resource	CI Sector	Risk Management	Government	Chamber of Commerce		Intermediate
Mobile Cybersecurity and the Internet of Things	PDF	https://api.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf	General Resource	CI Sector	Risk Management	Nonprofit	Cellular Telecommunications and Internet Association		Intermediate
Information Assurance and Security	PDF	https://www.cs.utexas.edu/~byoung/cs361c/slides1-intro.pdf	General Resource	CI Sector	Information Assurance	Nonprofit	University of Texas at Austin		Advanced
Information Assurance/Information Security; Computer System Security	PDF	https://csrc.nist.gov/CSRC/media/Events/CSSPAB-JUNE-2002-MEETING/documents/Lainhart-06-2002.pdf	General Resource	CI Sector	Information Assurance	Corporation	Pricewaterhouse Coopers		Advanced
Protecting Personal Information: A Guide for Business	PDF	https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf	Guide	CI Sector	Preparedness	Government	Federal Trade Commission		Beginner
Handling Destructive Malware	Website	https://www.us-cert.gov/ncas/tips/ST13-003	Guide	CI sector	Security Breaches	Government	United States Computer Emergency Readiness Team		Intermediate
Securing Network Infrastructure Devices	Website	https://www.us-cert.gov/ncas/tips/ST18-001	Guide	CI Sector	Risk Management	Government	United States Computer Emergency Readiness Team		Intermediate

Before You Connect a New Computer to the Internet	Website	https://www.us-cert.gov/ncas/tips/ST15-003	Guide	CI sector	Preparedness	Government	United States Computer Emergency Readiness Team	Beginner
2017 State of Cybersecurity Among Small Businesses in North America	PDF	https://bbbprograms.org/siteassets/documents/bbb-cybersecurity/cybersecurity_final_lores.pdf	Report	CI sector	Risk Assessment	Corporation	Better Business Bureau	Beginner
Multifactor Authentication for E-Commerce	PDF	https://www.nccoe.nist.gov/sites/default/files/library/sp1800/cr-mfa-nist-sp1800-17.pdf	Guide	CI sector	Risk Management	Government	National Institute of Standards and Technology	Advanced
2017 Annual Report	PDF	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf	Report	CI sector	Standards	Government	National Institute of Standards and Technology	Advanced
Cyber Risk in an Internet of Things World	Website/ PDF	https://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/cyber-risk-in-an-internet-of-things-world-emerging-trends.html	Guide	CI sector	Internet of Things	Corporation	Deloitte	Beginner
Internet of Things From Cybersecurity Perspective	PDF	https://www.theseus.fi/bitstream/handle/10024/151498/IoT%20from%20cyber%20security%20perspective.pdf?sequence=1&isAllowed=y	Report	CI sector	Internet of Things	Corporation	Theseus	Advanced
Demystifying Internet of Things Cybersecurity	PDF	https://www.iotca.org/wp-content/themes/iot/pdf/IoT-Cybersecurity-Alliance-Demystifying-IoT-Cybersecurity.pdf	Guide	CI sector	Internet of Things	Corporation	IoT Cybersecurity Alliance	Beginner
Common Cybersecurity Language	PDF	https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf	General Resource	CI sector	Preparedness	Government	US Department of Homeland Security	Beginner

Cybersecurity Regained: Preparing to Face Cyber Attacks	PDF	https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf	Report	CI sector	Preparedness	Corporation	Ernst and Young		Intermediate
IT Checklist for Small Businesses	PDF	https://www.cpaaustralia.com.au/~/media/corporate/allfiles/document/professional-resources/practice-management/it-checklist-for-small-business-new.pdf?la=en	Guide	CI sector	Preparedness	Non-profit	Certified Practicing Accountants Australia		Intermediate
Cybersecurity Implementation Guide for Small and Medium Sized Enterprises	PDF	https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf	Guide	CI sector	Risk Assessment	Non-profit	Center for Internet Security		Advanced
Cybersecurity Tech Basics: Vulnerability Management	PDF	https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf	General Resource	CI sector	Vulnerabilities	Non-profit	Center for Internet Security		Intermediate
Cyber Defense Challenges from the Small and Medium Sized Business Perspective	PDF	https://www.sans.org/reading-room/whitepapers/hsoffice/cyber-defense-challenges-small-medium-sized-business-perspective-38160	General Resource	CI sector	Vulnerabilities	Corporation	SANS		Intermediate
Managing Cybersecurity and e-Commerce Risks in Small Businesses	PDF	http://ibii-us.org/Journals/JMSBI/V2N1/Publish/V2N1_2.pdf	Guide	CI sector	Risk Management	Academic Institution	Texas Southern University		Intermediate

Small Business Cybersecurity Guide	PDF	https://www1.maine.gov/ag/docs/Small-Business-Cyber-Security-Guide.pdf	Guide	CI sector	Preparedness	Academic Institution	University of Southern Maine		Intermediate
Common Sense Guide to Cybersecurity for Small Businesses	PDF	https://www.uschamber.com/sites/default/files/legacy/reports/cybersecurityguide923.pdf	Guide	CI sector	Preparedness	Government	US Chamber of Commerce		Beginner
Maryland Personal Information Protection Act	Website	http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gcl&section=14-3504&ext=html&session=2018RS&tab=subject5	Law	CI sector	Security Breaches	Government	Maryland General Assembly		Beginner
Assessments: Cyber Resilience Review	Website	https://www.us-cert.gov/ccubedvp/assessments	General Resource	CI sector	Preparedness	Government	US Computer Emergency Readiness Team		
Small Firm Cybersecurity Checklist	Website	http://www.finra.org/industry/cybersecurity#checklist	General Resource	CI sector	Preparedness	Non-profit	Financial Industry Regulatory Authority		Intermediate
Incident Response Guide	PDF	https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf	Guide	CI sector	Security Breaches	Non-profit	Council for Registered Ethical Security Testers		Advanced
Incident Response Guide	PDF	https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf	Guide	CI sector	Security Breaches	Government	National Institute of Standards and Technology		Advanced
9 Questions to Ask Before Hiring a Managed Service Provider	Website	https://quickbooks.intuit.com/r/tech-review/9-questions-to-ask-before-hiring-a-managed-service-provider/	Guide	CI sector	Preparedness	Corporation	Intuit Quickbooks		Beginner
How to Hire and Evaluate Managed Security Service Providers (MSSPS)	Website	https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps	Guide	CI sector	Preparedness	Corporation	Digital Guardian		Beginner

Partnership for Workforce Quality (Grants and Support)	Website	http://commerce.maryland.gov/grow/partnership-for-workforce-quality-pwq	General Resource	CI sector	Preparedness	Government	State of Maryland		Beginner
Cybersecurity Awareness Training	PDF	https://www.hhs.gov/sites/default/files/fy18-cybersecurityawarenesstraining.pdf	Guide	CI sector	Preparedness	Government	U.S. Department of Health and Human Services		Intermediate
Securing Your Web Browser	Website	https://www.us-cert.gov/publications/securing-your-web-browser	Guide	CI sector	Preparedness	Government	US Computer Emergency Readiness Team		Beginner
Computer and Mobile Security	Website	https://www.consumer.ftc.gov/topics/online-security	Guide	CI sector	Preparedness	Government	Federal Trade Commission		Beginner
Antivirus Software Guide	Website	https://www.consumerreports.org/cro/antivirus-software.htm	Guide	CI sector	Preparedness	Corporation	Consumer R reports		Beginner
Secure Home Network	PDF	https://www.dni.gov/files/NCSC/documents/campaign/NSA-guide-Keeping-Home-Network-Secure.pdf	Guide	CI sector	Preparedness	Government	National Security Agency		Intermediate
Cyber Risk Management	Website	https://www.nist.gov/mep/cybersecurity-resources-manufacturers/cyber-risk-management	Guide	CI sector	Risk Management	Government	National Institute of Standards and Technology		Beginner
Internet Security Essentials for Business 2.0	Website	https://www.uschamber.com/Cybersecurity Essentials	General Resource	CI sector	Preparedness	Government	U.S. Chamber of Commerce		Intermediate
Cyber Crime - FBI Tips	Website	https://www.fbi.gov/investigate/cyber	General Resource	CI sector	Vulnerabilities	Government	Federal Bureau of Investigations		Beginner
IT Asset Management	PDF	https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5.pdf	General Resource	CI sector	Standards	Government	National Institute of Standards and Technology		Advanced
Information Sharing Groups	Website	https://www.isao.org/information-sharing-groups/	General Resource	CI sector	Vulnerabilities	International Organization	ISAO SO		Advanced
List of Information Sharing Organizations	Website	https://www.nationalisacs.org/member-isacs	General Resource	CI sector	Vulnerabilities	Nonprofit	National Council of ISACs		Advanced

Mutli-State Information Sharing & Analysis Center	Website	https://www.cisecurity.org/ms-isac/	General Resource	CI sector	Vulnerabilities	Nonprofit	Center for Internet Security		Advanced
Cybersecurity 101	PDF	https://www.dhs.gov/sites/default/files/publications/cybersecurity-101_4.pdf	General Resource	CI sector	Risk Management	Government	Department of Homeland Security		Beginner
Cyber Hygiene & Cyber Security Recommendations	PDF	https://www.secretservice.gov/forms/Cyber-Hygiene.pdf?n=11000	General Resource	CI sector	Preparedness	Government	U.S. Secret Service		Beginner