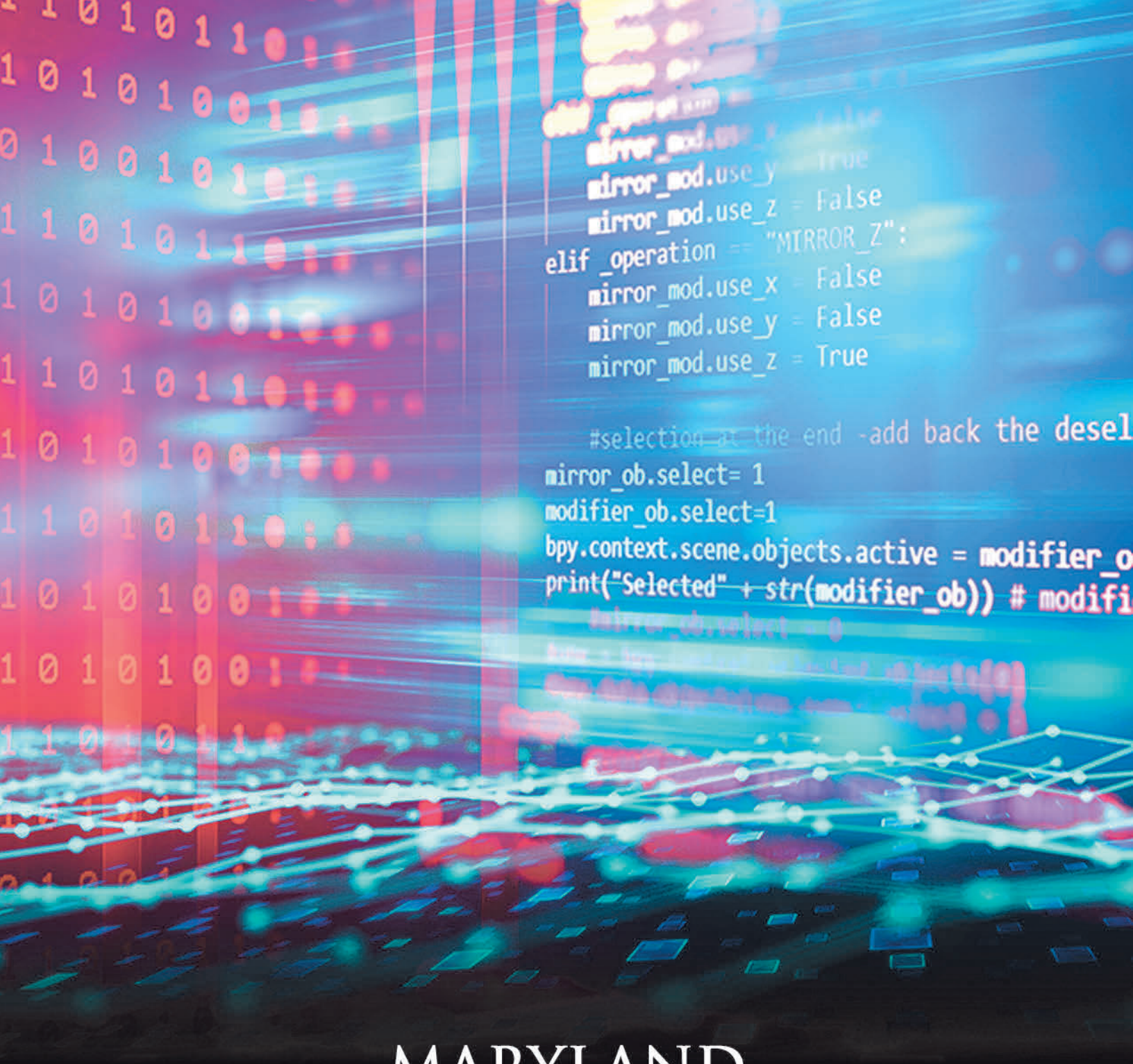

MARYLAND CYBERSECURITY COUNCIL ACTIVITIES REPORT 2019 - 2021

JULY 1, 2021

TABLE OF CONTENTS

SECTION		PAGE
I.	Statutory Requirement	2
II.	Executive Summary	2
III.	Council Organization and Membership	6
IV.	Council-Related Activities in Detail	12
V.	Setting the Stage for the Next Two Years	19
VI.	Conclusion	26
VII.	More Information	27
Appendix A. Consolidated Recommendations (2016 – 2021)		28
Appendix B. White Paper (An Information Sharing and Analysis Organization for Maryland)		33
Appendix C. Maryland Cybersecurity Council Members by Sector		55
Appendix D. Cybersecurity Sector Survey		62

I. Statutory Requirement

This is the third biennial activities report of the Maryland Cybersecurity Council covering FY 2020 and 2021. The report is required by SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 Section 3.[1] All Council reports, the Council's membership, its plenary and subcommittee meeting minutes, and various cybersecurity resources for consumers and small- and medium-size businesses may be found on the Council's website at https://www.umgc.edu/mdcybersecuritycouncil.

II. Executive Summary

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 in meeting federal cybersecurity guidance, to encourage and assist private sector firms to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to identify regulatory inconsistencies between State and Federal cybersecurity law that may complicate compliance by Maryland businesses, to support the creation of a cybersecurity resiliency plan for the State, and to recommend any other legislation to address cybersecurity issues.[2] In pursuing this charge, the Council informs legislation, undertakes educational and other public outreach initiatives, develops white papers and other work products, and fulfills duties required by other statutes.

Informing Legislation

During the last two years, the Council has continued to make policy recommendations intended for legislative consideration. With this report, the Council has 35 recommendations on record, including five new ones.[3] For the most part, these recommendations concern consumer protection, state and local government cybersecurity, criminal law, cyber education and workforce development, and the economic development of the State's cybersecurity sector.

This policy role is supported and extended by the Council's size, composition, and organization. Chaired by the Maryland Attorney General, Brian Frosh, the Council constitutes a crossroads linking many stakeholders from Maryland's public and private sectors. This provides it with a "real world" perspective on cybersecurity issues affecting the State, access to research that its members provide,[4] and practical proposals about how to address those issues.

The Council's composition ensures a nexus between its work and the General Assembly. By statutory design, the Council includes members of the State Senate and the House who in some cases lead or co-lead Council subcommittees. Each year, one or more of these members propose bills that would realize objectives of the Council's recommendations or would address other issues that have been described in the Council's activities reports. Moreover, as a matter 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] Md. Ann. Code Ann, St. Gov't Art. §9-2901 (J).
[3] See Appendix A for the cumulative recommendations of the Council. As indicated in the appendix, three of the 2021 recommendations update and replace three prior recommendations. The total (35) is net of these three.
[4] For example, see Appendix D.

course, other Council members are often willing to provide testimony in legislative committee hearings or to recommend others with expertise to do so.[5]

Council members who are also members of the General Assembly are Senator Susan Lee (District 16, Montgomery County), Senator Katie Fry Hester (District 9, Carroll and Howard Counties), Senator Bryan Simonaire (District 31, Anne Arundel County), Delegate Ned Carey (District 31A, Anne Arundel County), and Delegate Mary Ann Lisanti (District 34A, Harford County). Often these members are joined by other members of the General Assembly in their sponsorship of bills consistent with Council recommendations.

In the 2020 session, four of the Council's legislative members—Senator Lee, Senator Hester, Delegate Carey and Delegate Lisanti—cumulatively proposed nine bills (five of them cross-filed) that were aligned with the Council's recommendations and another three bills (two cross-filed) that aimed at other issues the Council has highlighted. However, because of the urgent priorities created by the pandemic and the abbreviated legislative session, none of these bills were passed.

Many of these bills were reintroduced in the 2021 session which lasted the full 90 days. Senator Lee, Senator Hester, Senator Simonaire, Delegate Carey, and Delegate Lisanti variously sponsored or co-sponsored seven bills (six cross-filed) that were connected with recommendations of the Council and three other bills (one cross-filed) that were responsive to issues that the Council had described. One of these three, proposed by Delegate Lisanti, would have expanded the responsibilities of the Council to include monitoring and evaluating the activities of certain agencies and proposing legislative changes where needed.

Two of these 2021 bills were passed by the General Assembly and approved by the Governor:

- *SB 623/HB 425* (*Criminal Law - Crimes Involving Computers*).[6] Sponsors**:** Senator Lee and Delegate Barron. Related Council recommendation: 2017 Recommendation 4. The law a) prohibits the knowing possession of ransomware except for certain purposes (e.g., research), b) establishes criminal penalties, c) in addition to other prohibited acts, specifically prohibits ransomware offenses "commit[ed] with the intent to interrupt or impair" the functioning of health care facilities or public schools, and d) changes monetary penalties for other computer-related offenses. SB 623/HB 425 follows previous efforts to pass legislation levying criminal penalties for the possession or use of ransomware in some form: 2017 (SB 287/HB 772), 2018 (SB 376/HB 456), and 2020 (SB 30/HB 215).

[5] Council members giving testimony include Dr. Anton Dahbura, Robert Day, Cyril Draffin, Dr. Anupam Joshi, Dr. Kevin Morgan, Markus Rauschecker, Laura Nelson, and Greg Smith (who also represented the Cybersecurity Association of Maryland). In addition, various "contributors" to the Council's work provided testimony in their own names: Joseph Carrigan, Dr. Loyce Pailen, Adjutant General (Ret) Dr. Linda Singh, and Ben Yelin, Esq. The Office of the Attorney General selectively supported bills (2021 SB 623/HB 425 and HB 587) and provided Letters of Information for others (2021 HB 1306, SB 69/HB 879).

[6] See https://mgaleg.maryland.gov/2021RS/chapters_noln/Ch_146_sb0623T.pdf

- *SB 49/HB 38* (*Department of Information Technology – Cybersecurity*).[7] Sponsors: Senator Lee and Delegate Carey. Related Council recommendation**:** 2019 Recommendation 2**.** This law expands the responsibilities of the Department of Information Technology to advise and oversee cybersecurity strategy across the executive branch of State government, as well as Maryland's public institutions of higher education and to provide nonbinding guidance about cybersecurity to the legislative and judicial branches, counties, municipalities, school systems, and all other political subdivisions of the State. The bill had been proposed in the 2020 session as SB 120/HB 235.

Outreach and Support

Beyond making policy recommendations intended for legislative consideration, the Council undertook other activities during the last two years.

- Annual cybersecurity policy event for members of the General Assembly. As an ongoing initiative, the Council organizes an annual luncheon in Annapolis at the beginning of each session with subject matter experts to discuss cybersecurity issues for legislators and their staff members. The Council's January 2020 reception included the Honorable George Barnes, Deputy Director of the NSA, who addressed election security and the major cybersecurity threats to the nation. In 2021, the speaker was the Honorable Suzanne Spaulding, former Under Secretary of the National Protection and Programs Directorate at the Department of Homeland Security (2011 – 2017), and the current Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Project at the Center for Strategic and International Studies. Ms. Spaulding, a Solarium Commission member, discussed the recommendations of the Commission with attention to the role of the states in the nation's cybersecurity. The 2021 event was virtual due to the pandemic.

- *Support for the Emergency Number Systems Board* (*ENSB*). Enacted in 2019, SB 339 (Public Safety – 911 Emergency Telephone System) directed the ENSB to consult with the Council on cybersecurity standards for the State's NextGen 911 system.[8] Pursuant to this responsibility, the Council's Subcommittee on Critical Infrastructure identified two subject matter experts[9] who have been advising ENSB's cybersecurity committee on standards. The Council's subcommittee has met twice with a representative of the ENSB committee to understand the NextGen 911 project and to receive updates on the committee's work.[10]

[7] See https://mgaleg.maryland.gov/2021RS/chapters_noln/Ch_318_sb0049E.pdf
[8] Md. Code Ann., Pub Safety Art, § 1-309.1 (A), at https://mgaleg.maryland.gov/2019RS/chapters_noln/Ch_302_sb0339E.pdf
[9] Dr. Michel Cukier (Associate Professor, University of Maryland and a member of the Council) and Mr. Marc Fruchtbaum (Adjunct Professor, University of Maryland Global Campus). See in this connection the minutes for the Council's June 10, 2020, plenary meeting at https://www.umgc.edu/documents/upload/draft-minutes-for-january-15-2021_A.pdf. Both Dr. Cukier and Mr. Fruchtbaum continue to be actively engaged with the standards drafting work.
[10] See subcommittee meeting minutes for April 3, 2020, and January 21, 2021.

- *Developing a plan for an Information Sharing and Analysis Organization* (*ISAO*) *for Maryland.* A white paper was drafted for the Council with subcommittee participation to describe how an ISAO could be established in the State.[11] The paper was responsive to the Council's 2019 Recommendation 4.[12]

- *Public education*. The Council's Subcommittee on Public and Community Outreach organized three webinars in the 2019 – 2021 period that were directed at general audiences and small businesses: *Cyber Criminals Are Looking for You* (April 30, 2020, and June 2, 2021) and *Cybersecurity and Your Business* (October 22, 2020). These webinars were hosted as a public service by Maryland CASH. Presenters included Attorney General Brian Frosh and Joseph Carrigan, Senior Security Engineer, Johns Hopkins University Information Security Institute.

- *Enhancement of the Council's repository of cybersecurity resources.* As a joint initiative of the Subcommittees on Critical Infrastructure and Public and Community Outreach, the Council launched a web-based searchable repository in 2017.[13] Consisting of curated resources on cybersecurity for critical infrastructure owners and operators as well as small- and medium-size businesses, and consumers, the repository averages about 30 – 40 visits per month. In the 2019 - 2021 period, another 150 resources were added to the repository, doubling its size. This was the result of recommendations by Council members and a legal intern at the University of Maryland Center for Health and Homeland Security at the University of Maryland Carey School of Law.[14] The repository is hosted and maintained by the University of Maryland Global Campus.

Setting the Stage for the Next Two Years

As part of its activities during the last two years, the Council has looked ahead to the next two. It will continue the core activities that it undertakes from year to year. But extending its agenda, it has adopted several new recommendations that may inform future bills of the Council's legislative members. Discussed in Section V below, these recommendations aim to enhance consumer protection, encourage cybersecurity practices among small businesses, and support workforce development of the cybersecurity sector in the State.

In addition, the Council is involved with two substantial studies to look at critical infrastructure within the State. The Council's enabling statute is especially concerned with critical infrastructure "damage or unauthorized cyber access" to which could threaten life on a large scale, cause "catastrophic economic damage" or "severe degradation of State or National

[11] See Appendix B.
[12] See Appendix A.
[13] Ibid., see Council 2016 Recommendations 8 and 17.
[14] During this biennial period, Michael Block, an intern at the Center for Health and Homeland Security at the University of Maryland School of Law, was responsible for compiling additional resources for the repository. Mr. Edward O'Donnell, Reference and Instruction Librarian at the University of Maryland Global Campus, maintains the repository for the Council.

security[.]"[15] To be completed within the next year, these studies are expected to result in further policy recommendations by the Council about certain critical infrastructure in the State:

- *The energy sector*. Working with the Council, the Office of the Attorney General (OAG) submitted a successful application to participate in the NSA's external fellowship program, a career enrichment program offered by the Agency to its employees. Specifically, the NSA agreed to place a fellow in OAG to work as a full-time analyst for one year on issues related to the cybersecurity of the utility sector serving Maryland. The role of the analyst is to inform the Attorney General's and the Council's understanding of a) the federal and State regulatory environment of utilities serving Maryland, b) how technologies such as drones and smart meters are affecting the security landscape, c) what steps other states have taken to enhance the cybersecurity and resilience of their utilities, and d) what policy initiatives could be implemented in Maryland to do the same.

- *State and local government.* Responsive to an increasingly aggressive threat environment, the Council will join a study of the cybersecurity needs of the State Executive Branch, counties, cities, and school districts.[16]

III. The Council's Organization and Membership

By statute, the Council is chaired by the Attorney General or the Attorney General's designee.[17] 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.[18] 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 on the Council are key federal agencies, State departments and agencies, including the State Board of Elections,[19] State legislators, and various sectors of Maryland civil society: critical infrastructure, higher education, the cybersecurity service sector, small businesses, statewide business and technology associations, and nonprofits, among others.[20] In 2019, with the advice and consent of the President of the Maryland Senate, the Attorney General appointed the Council's fifth elected state official, Senator Katie Fry Hester, co-chair of the General Assembly's Joint Committee on Cybersecurity, Information Technology, and Biotechnology. In

[15] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 (J)(2) and (J)(7).
[16] The project working group is co-led by Senator Katie Fry Hester and Ben Yelin at the Center for Health and Homeland Security (CHHS) at the university of Maryland School of Law, and includes Senator Susan Lee, Delegate Ned Carey and other members of the Maryland Cybersecurity Council and its staff, the Joint Committee on Cybersecurity, Information Technology, and Biotechnology; the Maryland State Department of Information Technology, the Maryland Emergency Management Agency, the Maryland Association of Counties, and student interns at CHHS.
[17] Ibid, §9-2901 (G).
[18] Ibid, §9-2901(C)-(F).
[19] SB 281. MD. Ann Code, St. Gov't Art. §9-2901, at https://mgaleg.maryland.gov/2018RS/chapters_noln/Ch_151_sb0281T.pdf
[20] For Council members grouped by sector, see Appendix C.

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.[21]

The Council's work was unimpaired by the pandemic. Like other State entities, it has continued to function virtually. Consequently, it has maintained a full schedule of plenary and subcommittee meetings.[22]

The Council meets in plenary session three times per year. These meetings are announced and open to the public. As part of its ongoing discovery, it dedicates half of its business meetings to presentations by subject matter experts on cybersecurity-related issues. Apart from the Annapolis meetings mentioned above, presenters at the plenary meetings in this biennial period included:

- Frank Grimmelmann (President and CEO, Arizona Threat Response Alliance [ACTRA]), "ACTRA Overview: Lessons Learned in Building a Successful State-level Threat Response Organization"
- The Honorable Tom Wheeler (FCC Chairman, 2013–2017) and RADM (USN, Ret.) and David Simpson (Chief, FCC Public Safety and Homeland Security Bureau, 2013–2017), "5G and Cybersecurity"
- Dr. Thomas Rid, Professor of Strategic Studies, Johns Hopkins University, "Active Measures: Hacking American Elections"
- Douglas Robinson, Executive Director, National Association of State CIOs (NASCIO) "Cybersecurity: the State of the States"

During the period of this report, the Council's subcommittees met a total of 20 times. Their meetings—also announced and open—shaped new recommendations discussed below and served as fora to obtain or request broader public input to inform bills. The latter has been true, for example, of the Subcommittee on Law, Policy, and Legislation (breach notification law updates, consumer control of their data, incentives for businesses to invest in cybersecurity)[23] and the Subcommittee on Cybersecurity Education and Workforce Development (talent pipeline management model for the State).[24]

The subcommittees also undertake other activities to advance Council recommendations. The white paper for an information sharing and analysis organization within the State was shaped by discussions between the Subcommittee on Critical Infrastructure and the Arizona Cyber Threat and Response Alliance.[25] Similarly, the public education webinars on cybersecurity topics mentioned earlier were organized by the Subcommittee on Public Awareness and Community Outreach.

---

[21] See Notes 5, 11, and 15.
[22] See Office of the Attorney General, *Open Meetings Act Manual* (10th edition), pp 3-5 to 3-7 at https://www.marylandattorneygeneral.gov/OpenGov%20Documents/omaManualPrint.pdf
[23] See the October 9, 2020, meeting minutes at https://www.umgc.edu/documents/upload/draft-minutes-for-october-9-2020.pdf.
[24] See the meeting minutes for November 13, 2020.
[25] See Appendix B.

Finally, subcommittee meetings sometimes surface issues that lead to policy discussions in other fora, such as when discussion of the "buy-Maryland" program within the Subcommittee on Economic Development led to a focus group of businesses with representatives of the State Commerce Department about how to improve the program.

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

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, Carey School of Law, University of Maryland, Baltimore
- Joseph Morales, Esq., Attorney, Maryland Hispanic Chamber of Commerce
- Jonathan Prutow, Project Manager, eGlobal Tech
- 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
- Create or enhance shared awareness of cyber vulnerabilities, threats, and incidents within the state
- Recommend best practices for developing a 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, Department of Information Technology (DoIT)
- Barry Boseman, Director, State and Local Affairs, National Security Agency, Liaison

to the Council

- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System
- Robert W. Day Sr., Councilman, College Park, Maryland
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Fred Hoover, Esq., Counsel, Maryland People's Counsel
- Linda Lamone, State 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, Board Member, Army Alliance
- Colonel William Pallozzi, Maryland Secretary of State Police
- Russell Strickland, Director, Maryland Emergency Management Agency

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, 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
- Cyril Draffin, Project Advisor to the Massachusetts Institute of Technology (MIT) Energy Initiative
- David Engel, Director, Maryland Coordination and Analysis Center
- Zuly Gonzalez, Co-Founder and CEO, Lightpoint Security
- Major General Timothy E. Gowen, Adjutant General, Maryland Military Department
- Michael Greenberger, Director, Center for Health and Homeland Security, Carey School of

Law, University of Maryland, Baltimore
- Terri Jo Hayes, Executive Consultant, Mfusion, Inc.
- Clay House, Vice President, Architecture, Planning, and Security, CareFirst
- Rajan Natarajan, CEO, QualityPro, Inc.

Subcommittee on Education and Workforce Development

Subcommittee Objectives

- Identify opportunities to enhance and support cyber workforce training and education in Maryland, including:
  - Recommendations for enhancing student interest in pursuing cybersecurity education; recommendations for developing programs for students and professionals entering the cybersecurity field
  - Recommendations for attracting teachers and faculty qualified to teach cybersecurity courses in high school and beyond
  - Recommendations for developing and modifying high school and higher education curricula to enhance cybersecurity skills and talent; recommendations for developing fundamental skills necessary for cybersecurity students and professionals
- Promote cyber research and development (R&D) in higher education, including recommendations on funding, incentivizing, or fostering collaboration in R&D
- Recommendations on improving pathways to employment in the cybersecurity field

Subcommittee Members

- Chair: Katie Fry Hester, Senator, District 9, Maryland General Assembly
- Dr. Michel Cukier, Associate Professor and Director, ACES, University of Maryland
- Stewart Edelstein, PhD, Executive Director, Universities at Shady Grove, University System of Maryland
- Anupam Joshi, PhD, Director, Center for Security Studies, University of Maryland, Baltimore County
- Miheer Khona, CEO Rising Sun Advisors
- Kevin Kornegay for David Wilson, EdD, President, Morgan State University
- Henry J. Muller, Director, Communications-Electronics Research, Development and Engineering Center, U.S. Army, Aberdeen Proving Ground
- Laura Nelson, President/CEO, National Cryptologic Foundation
- Rodney Petersen, Director, National Initiative for Cybersecurity Education, National Institute of Standards and Technology, Liaison to the Council
- Jonathan Powell, US Department of the Navy
- Bryan Simonaire, Senator, District 31, Maryland General Assembly

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.
- Vince Difrancisci, Senior Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- James Foster, CEO, Zerofox
- Don Fry, President and CEO, Greater Baltimore Committee
- Joseph Haskins Jr., Chairman, President, and CEO, Harbor Bank
- Brian Israel, Dixon Hughes Goodman LLP
- Mathew Lee, CEO, Fastech
- Brian Levine, Vice President, Technology and Innovation, Maryland Tech Council
- Christine Ross, CEO, Maryland Chamber of Commerce
- Gregg Smith, Chairman of the Board, Cybersecurity Association of Maryland (CAMI)
- Troy Stoval, CEO/Executive Director, Maryland Technology Development Corporation (TEDCO)
- Steven Tiller, Board Member, Fort 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, Executive Vice President, Myriddian, LLC

Council Staffing

The University of Maryland Global Campus is the staffing agency for the Maryland Cybersecurity Council.[26] 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. Council-Related Activities in Detail

Activities related to the Council include legislative and non-legislative initiatives, including outreach and support and stage setting activities. Each of these are discussed in turn. The stage setting activities are discussed in separate section.

Legislation Introduced by the Council's Legislative Members

The legislation discussed in this report are those undertaken by the Council's legislative members in connection with objectives of the Council. As noted in Section I, five members of the Council are also members of the General Assembly. This creates a bridge between the Council's policy work and the potential for enacting strong cybersecurity policies. As summarized below, the Council's legislative members proposed a total of 19 bills (seven cross-filed) and 16 bills (seven cross-filed), respectively, in the 2020 and 2021 sessions. Between both sessions, two bills (italicized/bold) passed the General Assembly and were approved by the Governor.

Bills Sponsored or Co-sponsored by Legislative Members of the Council				
	2020		2021	
	Bills Consistent with Objectives of Specific Council's Recommendations	Bills Addressing Challenges Discussed in the Council 2017 – 2019 Activity Report	Bills Consistent with Objectives of Specific Council's Recommendations	Bills Addressing Challenges Discussed in the 2017 – 2019 Activity Council Report
Government – Cybersecurity	SB 120/HB 235 SB 5 HB 996	SB 1036/HB 1618	***SB 49/HB 38*** SB 69/HB 879 SB 917/HB 587	SB 69/HB 879
Consumer Protection	SB 201/HB 237 SB 957/HB 784 HB 249 SB 443/HB 888		SB 112/HB 148 SB 930	
Changes in Criminal Law	SB 30/HB 215		***SB 623/HB 425***	
Cybersecurity Education & Workforce Development	SB 893	SB 1049 SB 724/HB 1580	SB 231/HB 824	SB 902
Election Security				HB 1306

Consumer Protection

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

The consumer-related cybersecurity bills introduced by the Council's legislative members in 2020 and 2021 would have realized three Council recommendations in some manner. These are to update the Maryland Personal Information Protection Act in tandem with changes in technology (2016 Recommendation 2), to expand consumer rights with respect to the data that firms collect and maintain (2017 Recommendations 3 and 7), and to take steps that would improve the cybersecurity of Internet of Things Devices (2017 Recommendation 6). Specifically, in the 2020 session, the bills aimed to:

- Expand the Maryland Personal Information Protection Act to include "activity tracking data" and "genetic information" as additional categories of data which could require consumer notification by a firm in the event of a breach and compress the timeline for consumer notification, among other changes. [SB 120/HB 237 (Commercial Law – Personal Information Protection Act) sponsored by Senator Lee and Delegates Carey, Charkoudian, Crosby, and C Watson.][27]

- Require businesses of a certain size to, among other things, advise consumers of the data collected about them, how the data is used, with whom the data is shared and why, and their right to request a copy of the information, to delete certain personal information, to opt out of third-party disclosure, and to provide notice to consumers about the collection of any additional data about them. [SB 957/HB 784 (Maryland Online Consumer Protection Act) sponsored by Senators Lee, Benson, and Lam and Delegates Carey and C. Watson.][28]

- Require businesses of a certain size to allow consumers to opt out of having their information shared in certain cases. [HB 249 (Consumer Protection – Right to Opt-out of Third-Party Disclosure) sponsored by Delegates C Watson and Carey.][29]

- Require manufacturers of "connected devices[,]" like home baby monitors, to incorporate elementary security safeguards to reduce their vulnerability to hacking [SB 443/HB 888 (Consumer Protection – Security Features for Connected Devices) sponsored by Senators Lee, Paterson, and Rosapepe and Delegates Carey and C Watson.][30]

In the 2021 session, Senator Lee and Delegate Carey sponsored SB 112/HB 148 (Personal Information Protection Act – Revisions), this time to add genetic information to the Act's definition of "personal information".[31] HB 148 passed the House with certain amendments and was referred to the Senate Finance Committee, which took no action on the bill. Additionally, the Maryland Online Consumer Protection Act was reintroduced by Senator Lee in 2021 (SB 930), which remained in the Senate Rules Committee until the end of session.[32]

---

[27] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0120/?ys=2020rs
[28] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0957/?ys=2020rs
[29] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/Hb0249/?ys=2020rs
[30] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0443/?ys=2020rs
[31] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0112
[32] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0930

Government Cybersecurity

As with consumer protection, the Council's legislative members sponsored bills that aligned with specific recommendations the Council made.

One of these bills was enacted in 2021. In 2019, the Council recommended that the State Department of Information Technology be chartered to advise the other branches of State government and political subdivisions about cybersecurity strategy and best practices (2019 Recommendation 2). To realize this recommendation, Senator Lee and Delegate Carey introduced SB 120/HB 235 (State Government – Department of Information Technology – Cybersecurity) in the 2020 session.[33] With 24 co-sponsors in the House, HB 235 passed with an amendment and was referred to the Senate Education, Health, and Environmental Affairs Committee where it remained until end of session. However, as mentioned earlier, in 2021 similar legislation was sponsored by Senator Lee and Delegate Carey (SB 49/HB 38), passed the General Assembly, and was approved by the Governor.[34]

Two other bills would have responded in some way to the Council's recommendation to create a "cyber first responder reserve" to augment capabilities of local jurisdictions in particular to prepare for and respond to an emergency (2016 Recommendation 1). In 2020, Senator Hester sponsored SB 5 (Public Safety - Cyber First Responder Reserve Established) to create a special unit within the State Military Department to do this.[35] In the same session, Delegate Lisanti sponsored HB 996 (Department of Information Technology – Cybersecurity Response Team) to help local jurisdictions develop emergency response plans and enter into mutual aid agreements.[36]

Finally, in 2020 and 2021, Senator Hester and Delegate Jackson sponsored bills which, while not aligned with specific recommendations made by the Council, were directed at local government cybersecurity challenges that the Council had identified in its 2017 – 2019 Activities Report.[37] These bills are as follows:

- In the 2020 session, SB 1036/HB 1618 (Maryland Emergency Management Agency - Cybersecurity Coordination and Operations Office – Establishment) would have a) expanded what constitutes an "Emergency" in the law to include cyber attacks, b) created and staffed a "cyber coordination and operations office" within MEMA to help improve "local, regional, and statewide cybersecurity readiness and response", and c) provided various support services to political subdivisions to improve their cybersecurity preparedness. The bills required the new office to consult with the State Department of Information Technology. SB

[33] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0120/?ys=2020rs
[34] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0049
[35] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0005/?ys=2020rs
[36] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0996/?ys=2020rs
[37] See 2017 – 2019 Activities Report of the Maryland Cybersecurity Council, pp. 15 ff, at https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf

1036 passed the Senate but remained within the House Health and Government Operations Committee until the legislative session ended.[38]

- In 2021, SB 69/HB 879 (Cybersecurity Coordination and Operations - Establishment and Reporting) was sponsored by Senators Hester and Simonaire and Delegate R. Watson. House and Senate versions of the bill were passed near the end of session but were not reconciled prior to session's end.[39] The bills changed substantially during session as a result of consultations with the State agencies involved and a working group convened by the Education, Health, and Environmental Affairs (EHEA) Committee to consider consolidating into one bill several bills concerned with State and local cybersecurity.

Consequently, the original SB 69/HB 879 absorbed the provisions of SB 917/HB 587 (Department of Information Technology - Status of Information Technology and Cybersecurity in State and Local Agencies) that had been sponsored by Senator Hester and Delegate R Watson[40] and SB 348 (State Government – Information Technology – Cybersecurity), a bill introduced by the Chair of the EHEA Committee at the request of the Department of Information Technology. The result was an amended SB 69/HB 879 that a) would have codified the organizational changes made in DoIT as a result of the Governor's Executive Order 01.01.2019.07, b) located responsibility for assisting political subdivisions with a "Director of Local Cybersecurity" within DoIT, and c) implemented various reporting requirements of State agencies and local units of government to DoIT.[41]

Changes in Criminal Law

As a deterrence measure, the Council has since 2016 recommended that the State criminalize ransomware and provide for increased penalties. In 2021, Senator Lee and Delegate Barron succeeded in realizing this recommendation with SB 623/HB 425 (Criminal Law - Crimes Involving Computers), which then passed the General Assembly with an amendment and was approved by the Governor.[42] This followed attempts in three prior sessions to pass a ransomware bill: 2017 (SB 287/HB 772), 2018 (SB 376/HB 456), and 2020 (SB 30/HB 215).

The 2021 bill was supported by the Office of the Attorney General, the Maryland Chiefs of Police and Maryland Sheriffs' Association, and the Maryland Hospital Association. It a) prohibits the knowing possession of ransomware except for certain purposes, b) establishes criminal penalties, c) in addition to other acts, specifically prohibits ransomware offenses that are "commit[ed] with the intent to interrupt or impair" the functioning of health care facilities or public schools, and d) changes monetary penalties for other computer-related offenses. The

[38] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB1036/?ys=2020rs
[39] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0069
[40] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0917
[41] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0348
[42] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0623

exception for knowing possession includes "a bona fide scientific, educational, governmental, testing, news, or other similar justification for possessing ransomware". [43]

Cybersecurity Education and Workforce Development

The Council has recommended requiring computer science and cybersecurity education in Maryland K12 schools (2016 Recommendation 10). In the 2020 session, Senator Hester proposed SB 893 (Public Health – Cyber Safety Handbook – Handbook Development and Publication),[44] and in the 2021 session she and Delegate P. Young sponsored SB 231/HB 824 (Public Schools –Cyber Safety Guide and Training Course –Development, Implementation, and Reporting).[45] The bills were meant to ensure an appropriate resource in public schools about the proper use of the internet and social media. The 2021 bills (SB 231/HB 824) were more extensive, requiring both the creation of a handbook and a self-guided training course, identifying with greater specificity the topics to be addressed, and requiring the separate training components for students, any school employee interacting with students, and parents. SB 893 passed the Senate only. SB 231/HB 824 did not advance beyond hearings in the Senate EHEA Committee and the House Ways and Means Committee.

More generally, the Council's 2017 – 2019 Activities Report noted that the persistent "shortfall in the number of needed professionals continues to be a defining characteristic of the cybersecurity industry… and [that] [a]s the nation's cyber epicenter, Maryland is affected by this shortage."[46] Senator Hester proposed several bills that were informed in part by the Council's Subcommittee on Cybersecurity Education and Workforce Development to respond to this need. While none of these bills passed the General Assembly, in one case the changes contemplated by a bill were subsequently implemented by the State anyway.

That bill was SB 724/HB 1580 (State Personnel - Information Technology and Cybersecurity Qualifications - Established (Maryland State IT Hiring Act).[47] Co-sponsored by Delegate Jackson, the bill reflected the recognition that many IT and cybersecurity practitioners have skills needed for job roles even if they do not have a degree and that stating job requirements in terms of skills would remove a barrier to filling open positions. Consequently, the bill would have required the State Department of Information Technology to define minimum qualifications for positions in terms of competencies—in this case referencing the NIST Cybersecurity Workforce Framework—with formal educational attainment used as a qualification only if established as a competency by the Framework. Since the introduction of this legislation in the 2020 legislative session, the State Department of IT has been in contact with the Maryland Department of Budget and Management to address the policy objectives raised by SB724/ HB1580.

[43] Md. Code Ann., Criminal Law Art, Section 7-302 (c)(5)(1), at https://mgaleg.maryland.gov/2021RS/chapters_noln/Ch_146_sb0623T.pdf
[44] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0893/?ys=2020rs
[45] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0231
[46] See 2017 – 2019 Activities Report of the Maryland Cybersecurity Council, p 17, at https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf
[47] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0724/?ys=2020rs

Senator Hester introduced two other bills in the 2020 and 2021 sessions that were responsive to the workforce gap described by the Council and informed by its Subcommittee on Cybersecurity Education and Workforce Development:

- SB 1049 (Cybersecurity Talent Pipeline Management Program).[48] Proposed in the 2020 session and modelled on the US Chamber of Commerce Talent Pipeline Management Program, SB 1049 would have created a public private "collaborative" to identify critical skills needs, develop a strategic plan to address those needs, and make specific recommendations to improve training offered through apprenticeships, entry-level positions, or postsecondary programs. The collaborative would be established via a competitive grant program administered and funded by TEDCO.

- SB 902 (Economic Development - Cyber Workforce Program and Fund – Established).[49] This 2021 bill retained the concept of a public/private partnership to guide existing and future investments in Maryland's cybersecurity workforce, but would have implemented it differently. Specifically, it would have created a "cyber workforce program" to be directed by the Department of Commerce "in consultation" with the Cybersecurity Association of Maryland (CAMI).

Under the latter bill, CAMI would have responsibility to provide "planning, strategies and other resources" to result in the development of new training programs where needed, the expansion of effective existing programs, the creation of programs to identify and screen individuals with an aptitude for cybersecurity careers, and to support training opportunities like apprenticeships and internships in cybersecurity. By design, unemployed Maryland residents identified by the Maryland Department of Labor would be a priority for screening and training opportunities. Funding for the program was to come from a "Cyber Workforce Fund" that would include any State appropriations, federal grants, and private donations. Amended during the committee process and passing the Senate, the bill was not passed by the full House prior to end of session.

Election Security

With the pandemic, there have been discussions within the Council's Subcommittee on Critical Infrastructure about the mechanics and security of the expanded option for absentee voting.[50] In the 2021 session, Delegate Lisanti proposed HB 1036 that would have chartered the Council in part to "monitor and evaluate the effectiveness of measures taken to ensure election security in the State" and to make recommendations accordingly.[51] The bill also included a similar direction to the Council in regard to "the status of high-speed internet" in the State. The House Ways and Means Committee held a hearing on the bill but did not vote on it.

[48] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB1049/?ys=2020rs
[49] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0902
[50] See meeting minutes for April 3, 2020.
[51] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB1306

Outreach and Support

Beyond the Council's role of making policy recommendations intended for legislative consideration, the Council undertook other activities in the last two years including:

- *Annual cybersecurity policy event for State legislators.* As an ongoing outreach initiative, the Council organizes 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 2020 reception included the Honorable George Barnes, Deputy Director of the NSA, who addressed election security and the major cybersecurity threats to the nation.[52] In 2021, the Honorable Suzanne Spaulding spoke about the recommendations of the Solarium Commission with attention to the states' role in the nation's cybersecurity.[53] Ms. Spaulding is the former Under Secretary of the National Protection and Programs Directorate at the Department of Homeland Security (2011 – 2017), and the current Senior Advisor for Homeland Security and Director of the Defending Democratic Institutions Project at the Center for Strategic and International Studies. She is a member of the Solarium Commission. The 2021 event was virtual due to the pandemic.

- *Subject Matter Expert Support for the Emergency Number Systems Board (ENSB).* Enacted in 2019, SB 339 (Public Safety – 911 Emergency Telephone System) directed ENSB to consult with the Council on cybersecurity standards for the State's NextGen 911 system.[54] Pursuant to its responsibility, the Council's Subcommittee on Critical Infrastructure identified two subject matter experts[55] who have been advising ENSB's cybersecurity committee on standards. The Council's subcommittee has met twice with a representative of the ENSB committee to understand the NextGen 911 project and to receive updates on the committee's work.[56]

- *Drafting of a white paper for a Maryland Information Sharing and Analysis Organization* (*ISAO*). The white paper is for the Council to address 2019 Recommendation 4.[57] The white paper evolved out of discussions involving members of the Subcommittee on Critical Infrastructure and Council staff with the Arizona Cyber Threat Response Alliance (ACTRA).[58] With the mobility of threats, the plan calls for a privately-led threat response organization across business sectors to promote threat sharing. The white paper proposes a partnership with ACTRA and discusses how such an ISAO could evolve to provide other services of value to the private sector in Maryland.[59]

---

[52] See Note 8.
[53] See Note 9.
[54] See Note 10.
[55] See Note 11.
[56] See Note 12.
[57] See Notes 13 and 14. See also the subcommittee meeting minutes for April 3, 2020 and the plenary Council meeting for June 9, 2021.See Appendix A for the 2019 Recommendation 4.
[58] For more information about ACTRA see https://www.actraaz.org/. ACTRA is listed with the ISAO Standards Organization at https://www.isao.org/information-sharing-group/geographic/arizona-cyber-threat-response-alliance-actra/
[59] See Appendix B.

- *Public education*. The Council's Subcommittee on Public and Community Outreach organized three webinars in the 2019 – 2021 period that were directed at general audiences and small businesses: *Cyber Criminals Are Looking for You* (April 30, 2020, and June 2, 2021) and *Cybersecurity and Your Business* (October 22, 2020). These webinars were hosted as a public service by Maryland CASH. Presenters included Attorney General Brian Frosh and Joseph Carrigan, Senior Security Engineer, Johns Hopkins University Information Security Institute.

- *Enhancement of the Council's repository of cybersecurity resources.* As a joint initiative of the Subcommittees on Critical Infrastructure and Public and Community Outreach, the Council launched a web-based searchable repository in 2017. Consisting of curated resources on cybersecurity for critical infrastructure owners and operators as well as small- and medium-size businesses, and consumers, the repository averages 30-40 visits per month. In the 2019 - 2021 period, another 150 resources were added to the repository, doubling its size. This was the result of recommendations by Council members and a legal intern at the University of Maryland Center for Health and Homeland Security at the University of Maryland Carey School of Law. The repository is hosted and maintained by the University of Maryland Global Campus.[60]

V. Setting the Stage for the Next Two Years

As part of its activity during the last two years, the Council has looked ahead to the next two. It will continue the core activities that it has undertaken from year to year. But the Council has extended its agenda by adopting several new recommendations and by undertaking, or participating in, two substantial studies that are expected to inform yet others.

<u>New Recommendations</u>

The Council has added five recommendations to those reflected in the two previous biennial reports.[61] Originating in its subcommittees, these new recommendations aim to enhance consumer protection, encourage cybersecurity practices among small businesses, require transparency about compromises of critical infrastructure, and support workforce development of the cybersecurity sector in the State.

Concerns about cybersecurity are universal, and the ways in which other states have attempted to address them are a valuable source of ideas and experience. This is particularly true of legislation in other states. Since 2015, the number of cybersecurity bills introduced in state legislatures has grown from 66 bills in at least 26 states to more than 250 bills in 44 states and Puerto Rico in

[60] See Notes 15 and 16.
[61] See Note 3.

2021.[62] Where appropriate, the discussion below references legislation introduced or enacted in other states.

Subcommittee on Law Policy and Legislation

2021 Recommendation 1. That the State consider incentives for businesses to assess their cybersecurity posture and to invest more, if necessary, to create a cybersecurity program consistent with recognized standards and frameworks.

This recommendation recognizes the statutory charge to the Council to "assist private sector cybersecurity businesses in adopting, adapting, and implementing the National Institute of Standards and Technology standards and practices[.]"[63]

A number of states have adopted *safe harbor* statutes to incent businesses to this end. The first state to do so for businesses in general was Ohio through the Ohio Data Protection Act (ODPA).[64] Effective November 2018, the ODPA extends the right of an affirmative defense in certain breach-related tort actions brought under Ohio law or in Ohio courts to firms that "create, maintain, and comply with a written cybersecurity program" that "reasonably conforms" with a statutorily recognized standard and that satisfy certain other requirements in the law. The ODPA includes the several key features. It:

Locates the determination of entitlement to the defense in State courts. The law does not implement a certification regime that would be undertaken by a State agency. State courts determine if a firm is entitled to the affirmative defense under the statute.

Avoids detailed prescription of security controls. Unlike other cybersecurity laws or regulations directed at particular business sectors[65], the ODPA links the entitlement to an affirmative defense to reasonable conformity with one or a combination of recognized frameworks and standards that the statute identifies. These include those published by NIST, the FedRAMP security assessment framework, the Center for Internet Security critical security controls, the ISO 2700 family of controls, and specialized regulatory regimes described below. This provides firms with a number

[62] For 2015 and 2021 data respectively, see National Council of State Legislatures annual cybersecurity summary at https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2015.aspx and https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx. For an analysis of federal and state legislation in 2020, see Garcia, M., Rauschecker, M., and von Lehmen, G. (2021, March 24). "An analysis of cybersecurity legislation: Congress, the States, Maryland". Presentation at CyberMaryland 2021. https://s3.amazonaws.com/bizzabo.file.upload/IwI5U7ZsQtid7yRInVMr_An%20Analysis%20of%20Legislation%20-%20Weds%20March%2024%200900%20-%20Show%20Time%20Deck.pdf

[63] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 (J)(4).

[64] 2018 SB 220, at https://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_132/bills/sb220/EN/05/sb220_05_EN?format=pdf. For a discussion of ODPA, see D. Hirsch, Keir Lamont, and Brian Ray, opus cit..

[65] For example, see Indiana HB 1372 (An Act to Amend the Indiana Code Concerning Insurance), Chapter 27 (Insurance Data Security), which was enacted and is effective June 30, 2021, http://iga.in.gov/static-documents/6/3/5/1/6351a8b8/HB1372.05.ENRS.pdf. On May 25, 2021, members of the Maryland Cybersecurity Council, Council staff, and representatives of the Office of the Maryland Attorney General discussed Ohio's experience with the law in a Zoom meeting with members of CyberOhio, then an advisory board to the State's attorney general, who were involved in shaping the legislation.

of defined options and avoids a static set of requirements that the State would need to update from time to time. Under the statute, businesses must respond directly to changes in the standards or frameworks by the issuing organizations.

Takes into account other regulatory regimes. The Act allows that a qualifying cybersecurity program may be achieved by firms already in substantial compliance with the Health Insurance Portability and Accountability Act (HIPPA), the Gramm-Leach-Bliley Act (GLBA), Federal Information Security Modernization Act, or the Health Information Technology for Economic and Clinical Health Act (HITECH). The statute requires that businesses in compliance with payment card industry (PCI) data security standard must also comply with one of the other standards that the ODPA lists.

Recognizes that one size does not fit all. The Act requires firms to "(c)reate, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection" in reasonable conformity with one or a more of the standards or frameworks that it identifies. But it allows that a firms program is "appropriate" if it is based on (1) the size and complexity of the covered entity; (2) the nature and scope of the activities of the covered entity; (3) the sensitivity of the information to be protected; (4) the cost and availability of tools to improve information security and reduce vulnerabilities; (5) the resources available to the covered entity."

Utah enacted a similar law (HB 80)[66] in 2021 and other state legislatures have seen the introduction of similar if not identical bills this year. These include Illinois (HB 3030),[67] New Jersey (SB 3062),[68] and Connecticut (HB 6607).[69] Georgia saw a similar bill (HB 240), although it did not link the qualifying cybersecurity program to a recognized standard ala the Ohio law.[70] Indiana enacted a statute that extends safe harbor against certain tort actions to insurance companies, again without using the standards approach. A 2021 Connecticut bill would have applied the safe harbor concept differently, providing a tax credit to businesses for certain investments in a cybersecurity program.[71]

2021 Recommendation 2. That the State consider appropriate legislation to ensure the transparency to consumers of the information held by entities about them and how it is used, the right of consumers to inspect, correct and delete such data, and their right to opt out of the sale of data to third parties.

---

[66] 2021 Utah HB 80 (Data Security Amendments), https://le.utah.gov/~2021/bills/hbillenr/HB0080.pdf
[67] 2021 Illinois HB 3030 (Cybersecurity Compliance Act), https://www.ilga.gov/legislation/102/HB/PDF/10200HB3030lv.pdf
[68] 2021 New Jersey SB 3062 (Affirmative Defense for Certain Breaches) https://www.njleg.state.nj.us/2020/Bills/S3500/3062_I1.PDF
[69] 2021 Connecticut HB 6607 (An Act Incentivizing Adoption of Cybersecurity Standards for Business), https://www.cga.ct.gov/searchresults.asp?cx=005177121039084408563%3Ahs1zq3ague8&ie=UTF-8&cof=FORID%3A10&q=HB6607&submission=%EF%80%82
[70] 2021 Georgia HB 260, https://www.legis.ga.gov/api/legislation/document/20212022/196593
[71] 2021 Connecticut HB 6161 (An Act Creating a Tax Safe Harbor for Organizations that Adopt a Written Cybersecurity Plan), https://www.cga.ct.gov/2021/TOB/H/PDF/2021HB-06161-R00-HB.PDF

This recommendation broadens and replaces a recommendation previously made by the Subcommittee that only addressed Internet Service Providers (ISPs).[72] The revised recommendation acknowledges that appropriate legislation may consider the size of an entity, the number of consumers on whom data is collected, the obligations otherwise in law to retain certain data, and whether certain data is already regulated, among other factors.

Superseding a previous recommendation, this reformulation takes into account the pace, scale, and ever-expanding practice of collecting ever deeper information about consumers' lives. The premise of the recommendation is that greater consumer awareness and control over data will produce two potential benefits.

One is possibly reducing the volume of sensitive data exposed in the improper disclosure of information through breaches. As Maryland residents know, breaches affecting them are a fact of life. In Fiscal Year 2020, 871 unique entities—businesses, nonprofits, units of government—reported breaches impacting Maryland residents. The cumulative number of residents whose data was compromised was 630,867. Since each entity reports breaches separately, this number likely includes some number of residents more than once, indicating that some residents were affected by more than one breach. This is even more probable considered longitudinally where the cumulative number of separately reported Maryland residents affected in three fiscal year snapshots (2016, 2018, and 2020) is more than 5.2 million.[73]

The other benefit of greater transparency and consumer control over data is to help entities avoid unfair outcomes. In 2019 testimony before the US Senate Committee on Banking, Housing, and Urban Affairs, the executive director of the World Privacy Forum stated that:

1) Credit scores and predictions are being sold that are not regulated by the Fair Credit Reporting Act (FCRA);
2) The technology environment is facilitating more scores being used in more places in consumers' lives, and not all uses are positive;
3) These scores are created without due process for consumers; and
4) These scores can cause consumers exceptional harm.[74]

[72] See 2017 – 2019 Activities Report of the Maryland Cybersecurity Council, Appendix A, 2017 Recommendation 3, https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf

[73] See three reports published by the Office of the Maryland Attorney General Identity Theft Program: *Data breaches: FY 2016 snapshot* (https://www.umgc.edu/documents/upload/data-breaches-fy-2016-snapshot.pdf), *Data breaches: FY 2018 snapshot* (https://www.umgc.edu/documents/upload/data-breaches-fy-2018-snapshot.pdf) and d*ata breaches: FY 2020 snapshot* (https://www.umgc.edu/documents/upload/data-breaches-fy-2020-snapshot-pdf.pdf)

[74] Dixon, P (2019, June 6). *Data brokers, privacy, and the fair credit reporting act*. Testimony before the US Senate Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/imo/media/doc/Dixon%20Testimony%206-11-19.pdf

In the same hearing, the Government Accounting Office provided similar testimony highlighting gaps in federal law that have not paced with contemporary practices in the collection and use of consumer data presenting the potential for unfair outcomes.[75]

In the absence of federal law providing greater transparency and control, California enacted its Consumer Privacy Act in 2018, which was amended in 2019, and again in 2020.[76] Virginia has followed suit with its own Consumer Data Protection Act in 2021.[77] While similar in many ways to the California law, it was influenced by a bill introduced this year in the Washington State General Assembly that did not pass.[78]

2021 Recommendation 3. That the State consider legislation to enhance the security of Internet of Things (IoT) devices.

This recommendation generalizes 2017 Recommendation 6 to recognize that there are a variety of approaches to improving the cybersecurity of IoT devices.

Two states have enacted laws to enhance the security of such devices. In 2018, California was the first to require security basic features in IoT devices "sold or offered for sale" in the State.[79] The law requires "connected" devices to have security features that are "appropriate to the nature and function of the device; appropriate to the information the device may collect, contain or transmit; and designed to protect the device and any information contained in it from unauthorized access, destruction, use, modification, or disclosure[.]" For devices equipped for authentication outside of a local area network, the security requirements of the Act are met if passwords that are pre-programmed are unique, or the consumer is required to generate a password before the device can be accessed the first time. Oregon passed a law in 2019 that is modelled on California's but with a number of differences.[80]

Attempts have been made in Maryland and other states to pass bills that are identical or similar to the California law. In the 2019 and 2020 sessions, Senator Lee and Delegate Carey sponsored

---

[75] Cackley, A.P. (2019, June 11). *Consumer privacy: Changes to legal framework needed to address gaps.* Statement of the Government Accounting Office in testimony before the US Senate Committee on Banking, Housing, and Urban Affairs. https://www.banking.senate.gov/imo/media/doc/Cackley%20Testimony%206-11-19.pdf

[76] See Office of Governor Gavin Newsome. (2019, October 11*). Governor Newsome issues legislative update* 10-11-19. https://www.gov.ca.gov/2019/10/11/governor-newsom-issues-legislative-update-10-11-19/ and Cole, C., Baker, M., and Burgess, K. (2020, November 16). *Move over, CCPA: The California Privacy Rights Act gets the spotlight now*. Bloomberg Law. https://news.bloomberglaw.com/privacy-and-data-security/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now.

[77] 2021 HB 2307, https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0035+pdf. For an overview of the Virginia law, see Rippy, S. (2021, March 3). *Virginia passes the Consumer Data Protection Act*. iapp. https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/

[78] 2021 Washington State SB 5062, https://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062.pdf?q=20210531110142

[79] 2018 California AB 1906 (Information Privacy: Connected Devices), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB1906. The law was effective January 1, 2020.

[80] 2019 Oregon HB 2395, https://olis.leg.state.or.us/liz/2019R1/Downloads/MeasureDocument/HB2395/Enrolled

SB 553/HB 176 and SB 443/HB 888, respectively. Other states that have tried to enact such laws recently include Illinois, Massachusetts, New York, and Virginia.[81]

A key development affecting this recommendation will be the broader industry impact of HR 1668 (Internet of Things Cybersecurity Improvement Act of 2020) passed by the 116th Congress and signed by the President. With certain limitations, the Act requires that federal agencies only procure connected devices that meet NIST IoT security requirements.[82] Similarly, it will bear watching whether the security labelling pilot directed by Executive Order 14028 for consumer IoT devices will be adopted by software developers and manufacturers.[83]

2021 Recommendation 4. That there be transparency with the State by critical infrastructure providers about compromises that interfere with operations.

Georgia enacted a broad reporting law[84] relating to breaches this year that applies to all branches of state government, political subdivisions, any other "authority" established under State law, and to utilities. Utilities include any "publicly, privately, or cooperatively owned line, facility, or system for producing, transmitting, or distributing power, electricity, light, heat, or gas." Reports are to be made to the State Director of Emergency Management and Homeland Security or a designee.

Under the statute, public authorities must report any compromise "determined by the director to be the type of cyber attack, data breach, or use of malware to create a life-safety event, substantially impact the security of data and information systems, or affect critical systems, equipment, or service delivery." If the compromise is of such a nature that a public entity must report it to the US Government, the entity meets the statute's reporting requirement by providing substantially the same information to the Director; "provided, however, if such information is prohibited under any federal law, rule, or regulation from being disseminated, the utility shall provide such information upon the expiration or lifting of such prohibition."

Subcommittee on Cybersecurity Workforce Development

2021 Recommendation 5. That the State consider a strategic partnership a) to engage business and industry in identifying gaps in IT/cybersecurity workforce development and in defining training requirements; b) to leverage the postsecondary sector and other training and education providers to offer needed training; c) to coordinate upskilling opportunities for the unemployed or underemployed; and d) to provide enhanced funding

---

[81] See Quinnell, R. (2021, January 5*). Legal requirements for IoT security start to emerge*. EDN. https://www.edn.com/legal-requirements-for-iot-security-start-to-emerge/

[82] See 2020 HR 1668 at https://www.govinfo.gov/content/pkg/BILLS-116hr1668enr/pdf/BILLS-116hr1668enr.pdf For an overview of publications developed pursuant to the law to provide guidance about IoT security, see National Institute of Standards and Technology. (2020, December 15). *NIST releases draft guidance on Internet of Things device cybersecurity*. (Press Release). https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity.

[83] See Executive Order 14028 (Improving the Nation's Cybersecurity) issued May 21, 2021, Section 4 (s). https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf

[84] See 2021 Georgia HB 156 at https://www.legis.ga.gov/api/legislation/document/20212022/200290.

for a variety of pathways to the cybersecurity profession, including apprenticeships and career and technical education.

Maryland ranks as a top ten "tech" state by several measures, but it is challenged to find the skilled workers that it needs. This is especially true in cybersecurity.

"Net tech" as an employment metric that *CompTIA* uses to gauge how dominant the tech sector is within a state. "Net tech" employment includes core technical workers, whether with a company or full-time self-employed, and other nontechnical workers (sales, marketing, HR, etc.) who round out the workforce of technical firms.[85]

Among US states, Maryland has the sixth highest concentration of "net tech" workers as a percentage (10.7%) of the State's total employment.[86] Among US cities, Baltimore ranks 20th in "net tech" employment.[87] This sector accounts for 12.2% ($44.7 billion) of Maryland's economy, and it is expected to grow by 16% over the 2020 – 2030 period.[88]

Within its tech sector, Maryland has continued to see a persistent shortfall in cybersecurity related talent. According to *Cyberseek*, from April 2020 – March 2021, the State had 41,708 professionals employed in cybersecurity positions but also had 19,545 open positions.[89] The same is the case across the nation, putting Maryland in competition with other states for talent. This is true despite the State's strong postsecondary education sector and a number of complementary workforce development initiatives.

This recommendation was informed by subcommittee discussions that explored the talent pipeline management model employed by Kentucky, Arizona and other states that is premised on industry-led discussions of workforce training needs. It also benefitted from a survey that was conducted earlier this year by the Cybersecurity Association of Maryland (CAMI) and co-developed with the subcommittee and Council staff.[90]

The survey was directed to the more than five hundred Maryland firms belonging to CAMI. Seventy-one responses were received, most (79%) representing firms with 100 employees or less. In general, the findings mirror those of national surveys. A majority (70%) state that it is somewhat or extremely difficult to find the talent in Maryland that they need. The hardest to fill positions are those connected with cloud security and network security. Almost half of the respondents (48.6%) reported that new professionals hired lacked technical skills core to their job role. The survey revealed support for apprenticeship and intern programs with 40.3% stating that they would be willing to support apprenticeships and 30.6% virtual internships for college students. One comment received as part of the survey raised the question whether State support

[85] CompTia. (2021, March). *Cyberstates* 2021. (p 5). https://www.cyberstates.org/pdf/CompTIA_Cyberstates_2021.pdf
[86] Ibid, pp. 12, 38.
[87] Ibid, Appendix A.5, p. 126.
[88] Ibid, pp. 12, 38, 143 (Appendix D.3).
[89] See Cyberseek (https://www.cyberseek.org/heatmap.html)
[90] See Appendix D.

for apprenticeships is enough, suggesting that tuition support for apprentices taking college courses should also be considered.

Two Studies to Be Completed in FY 2022

In addition to new recommendations that will receive attention in the next two years, the Council is involved in two substantial studies to look at critical infrastructure within the State. The Council's enabling statute is especially concerned with critical infrastructure "damage or unauthorized cyber access" which could threaten life on a large scale, cause "catastrophic economic damage" or "severe degradation of State or National security".[91] To be completed within the next year, these studies are expected to result in further policy recommendations by the Council about certain critical infrastructure in the State:

- *The energy sector*. Working with the Council, the Office of the Attorney General (OAG) submitted a successful application to participate in the NSA's external fellowship program, a career enrichment program offered by the Agency to its employees. Specifically, the NSA agreed to place a fellow in OAG to work as a full-time analyst for one year on issues related to the cybersecurity of the utility sector serving Maryland. The role of the analyst is to inform the Attorney General's and the Council's understanding of a) the federal and State regulatory environment of utilities serving Maryland, b) how technologies such as drones and smart meters are affecting the security landscape, c) what steps other states have taken to enhance the cybersecurity and resilience of their utilities, and d) what policy initiatives could be implemented in Maryland to do the same.

- *State and local government.* Responsive to an increasingly aggressive threat environment, the Council will join a study of the cybersecurity needs of the State Executive Branch, counties, cities, and school districts.[92]

VI. Conclusion

By statute, the Maryland Cybersecurity Council embodies a "whole of community" approach to cybersecurity issues affecting the State. At nearly 60 members, its membership cuts across the public and private sectors. This breadth keeps the Council focused on the range of cybersecurity-related issues important to the State and its residents.

These issues concern consumer protection, state and local government cybersecurity, criminal law, cyber education and workforce development, and the economic development of the State's cybersecurity sector. The Council's contribution includes recommendations that inform legislation; public education, outreach, and support activities; and participation in studies that yield insight into ways to further enhance the cybersecurity and resiliency of the State. The

[91] SB 542. Md. Ann. Code, St. Gov't Art. §9-2901 (J)(2) and (J)(7).
[92] See Note 18.

Council's meetings are public, and it welcomes the participation of everyone who has an interest in these issues.[93]

VII. 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@umgc.edu[94]

[93] Meetings are announced on the Council's website.
[94] The Report was offered to the Council for review. Suggested changes were received from members of each subcommittee and were incorporated into the draft. The Report was subsequently reviewed and approved by the Office of the Attorney General. The draft was created by Dr. Gregory von Lehmen, Special Assistant for Cybersecurity, University of Maryland Global Campus, and staff to the Maryland Cybersecurity Council.

APPENDIX A

Recommendations of the Maryland Cybersecurity Council

2016 - 2021

Recommendations in the 2016 Interim Report		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

Recommendations in the 2017 Biennial Report		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. (Replaced 2021 Recommendation 2).	Law, Policy, and Legislation

	Recommendations in the 2017 Biennial Report (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. (Replaced by 2021 Recommendation 3).	
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. (Replaced by 2019 Recommendation 4).	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. 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.	Cyber Operations and Incident Response Subcommittee

Recommendations in the 2019 Biennial Report		Originating Subcommittee
1.	The state should address the security vulnerabilities of its absentee balloting system as soon as possible.	Joint Recommendation of Law, Policy, Legislation Subcommittee and Critical Infrastructure Subcommittee
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 within the state.	Law, Policy, and Legislation
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.	Critical Infrastructure Subcommittee
4	*Information Sharing and Analysis Organization (ISAO).* The state should establish or facilitate an information sharing and analysis organization especially targeted on 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 proactive training. There are different models that state policymakers can consult for this purpose. (Replaces 2017 Recommendation 8).	Joint Recommendation of the Critical Infrastructure Subcommittee and the Economic Development Subcommittee
5.	*Cybersecurity Workforce Development.* The state 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) 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.	Economic Development
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.	
7.	*Implementing a tax credit analysis in coordination with the Maryland Department of Commerce to review of existing tax credits.* The objective is 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, 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.	

Recommendations in the 2021 Biennial Report		Originating Subcommittee
1.	That the State consider incentives for businesses to assess their cybersecurity posture and to invest more, if necessary, to create a cybersecurity program consistent with recognized standards and frameworks.	Law, Policy, Legislation
2.	That the State consider appropriate legislation to ensure the transparency to consumers of the information held by entities about them and how it is used, the right of consumers to inspect, correct and delete such data, and their right to opt out of the sale of data to third parties. (Replaces 2017 Recommendation 3)	
3.	That the State consider legislation to enhance the security of Internet of Things (IoT) devices. (Replaces 2017 Recommendation 6)	
4.	That there be transparency with the State by critical infrastructure providers about compromises that interfere with operations.	
5.	That the State consider a strategic partnership a) to engage business and industry in identifying gaps in IT/cybersecurity workforce development and in defining training requirements; b) to leverage the postsecondary sector and other training and education providers to offer needed training; c) to coordinate upskilling opportunities for the unemployed or underemployed; and d) to provide enhanced funding for a variety of pathways to the cybersecurity profession, including apprenticeships and career and technical education.	Cybersecurity Education and Workforce Development

APPENDIX B

WHITE PAPER
AN INFORMATION AND ANALYSIS ORGANIZATION FOR MARYLAND

DOCUMENT FOR THE MARYLAND CYBERSECURITY COUNCIL
FROM THE SUBCOMMITTEE ON CRITICAL INFRASTRUCTURE
IN SUPPORT OF
COUNCIL 2019 RECOMMENDATION 4

JUNE 9, 2021

White Paper[95]
An Information Sharing and Analysis Organization for Maryland

I. The Vision

Proposed is a grass-roots, industry-created, industry-led, and wholly membership-funded Maryland Information Sharing and Analysis Organization (ISAO).[96] The current cyber threat environment requires coordination and collaboration by communities of interest that complement Information Sharing and Analysis Centers (ISACs), which were primarily established to focus on protecting the Nation's critical infrastructure (CI). ISAOs are meant to do that; widen threat sharing by bringing together entities that cross CI sectors and include non-CI entities. As ISAOs have been stood up, they have been used for cyber workforce development and other objectives beneficial to their members.

While large Maryland CI firms participate in their sector-specific ISACS, there is no threat sharing organization in the State that has been able to effectively bring together representatives from across various CI and non-CI sectors. Moreover, smaller CI providers in Maryland—water co-ops are an example—are not likely to participate in their sector ISACs and most likely operate outside of any organized threat sharing network.

Central to this proposal is both an *ask and a unique offer of assistance*.

- The ask is for a small group of firms—six—that would be strongly committed from Day 1 through their financial support to stand up the ISAO, to take an active part in shaping its organization, and to set it on a trajectory of success.
- The offer of assistance is from the Arizona Cyber Threat Sharing Alliance (ACTRA)—a well-established and nationally-respected ISAO. ACTRA is willing to support the stand-up of a Maryland ISAO so that there is immediate value to the Maryland charter firms. This would be in terms of cross-sector threat sharing, access to ACTRA's organizational and operational documents to adapt to Maryland, and in general an insider's seat to experience the range of cyber workforce development and other ACTRA activities.

To be emphasized is that the proposal is not simply to replicate ACTRA. It is to draw on its culture, organization, and operational experience as appropriate to launch a uniquely Maryland entity. The ways in which ACTRA is willing to assist is discussed in Section V below.

---

[95] This working document was drafted by Dr. Gregory von Lehmen for the Subcommittee on Critical Infrastructure of the Maryland Cybersecurity Council. It includes as an appendix a legal analysis by interns at the Center for Health and Homeland Security at the University of Maryland School of Law. The representations about ACTRA have been made with the approval of Frank Grimmelmann, ACTRA President/CEO.

[96] The need for ISAOs was recognized by Executive Order 13691 (Promoting Private Sector Information Sharing), accessed at https://www.govinfo.gov/content/pkg/FR-2015-02-20/pdf/2015-03714.pdf. For a discussion of ISACS and ISAOS see Bruce Bakis and Edward Wang, *Building a National Cyber Information Sharing Ecosystem*, MITRE Corporation, 2017, accessed at https://www.mitre.org/sites/default/files/publications/building-national-cyber-information-sharing-ecosystem-pr-17-1125.pdf

II. Legal Protections for Threat Information Sharing

The proposal presumes certain protections for firms engaged in sharing threat information. Under federal law, firms sharing threat information according to law are afforded protections against:

- Tort litigation
- State and local disclosure laws, including FOIA requests
- Government enforcement actions as a result of breach disclosure
- Disclosure of Intellectual Property and Trade Secret Information
- Government antitrust enforcement actions

A detailed analysis of the applicable law by the Center for Health and Homeland Security (CHHS) at the University of Maryland-Baltimore School of Law may be found in Appendix B.

III. The Model

There is no one model for ISAOs. "ISAOs may be organized on the basis of sector, sub-sector, region, or any other affinity, including in response to particular emerging threats or vulnerabilities. ISAO membership may be drawn from the public or private sectors or consist of a combination of public and private sector organizations. ISAOs may be formed as for-profit or nonprofit entities."[97]

The proposed model for a Maryland ISAO is a proven state-level one, namely the Arizona Cyber Threat Response Alliance (ACTRA). ACTRA is a 501 (3)(c). It was created in 2013 after an 18-month long study that began in 2011. With the support of the Arizona InfraGard, ACTRA was established "to be an affiliated non-profit entity to serve as the self-governed private-sector-controlled hub for cyber information exchange and response".[98] Because of ACTRA's success, it has been held up as a national model and has already been replicated in the Wisconsin Cyber Threat Response Alliance (WICTRA).[99]

Discussions with ACTRA inform this proposal. It began with a presentation to the Maryland Cybersecurity Council last October by ACTRA CEO, Frank Grimmelmann.[100] Following Mr.

---

[97] EO 13691 Section 2 (b). For a discussion of different models, see ISAO 600-1, *A Framework for State-level Sharing and Analysis Organizations*, ISAO Standards Organization: June11, 2018 (Ver 1.0), p 23ff, accessed at https://www.isao.org/storage/2018/06/ISAO-600-1-A-Framework-for-State-level-ISAOs.pdf

[98] See ACTRA's history at https://azinfragard.org/actra/

[99] See Appendix C which is excerpted from Natasha Cohen and Brian Nussbaum, *Cybersecurity for the States: Lessons from Across America*, New America, May 2018, See pp 30-31, Chapter 2, and Appendix I, accessed at https://d1y8sb8igg2f8e.cloudfront.net/documents/Cybersecurity_for_the_States_Lessons_from_Across_America_FINAL_3.pdf. More information about WICTRA can be found at https://sites.google.com/wictra.org/wictra/about-us

[100] The Maryland Cybersecurity Council is a statutory body of nearly 60 members—private and public sector representatives—that is chaired by the Maryland Attorney General. More information about the Council can be found at http://www.umuc.edu/mdcybersecuritycouncil Mr. Grimmelmann is the founding President/CEO of

Grimmelmann's presentation, members of the Council visited Phoenix for a day of meetings with ACTRA staff, selected ACTRA corporate members, and other stakeholders. In those conversations, ACTRA offered three different options for assisting the launch and operation of a Maryland ISAO. These play a critical part in this proposal and are discussed under Section V below.

IV. The Business Case for a Maryland ISAO

First, an ISAO could greatly enrich the actionable threat-sharing ecosystem within the private sector in the State in at least three ways.

- It would broaden the threat sharing network by including CI and non-CI firms, thereby enhancing awareness and increasing the actionable threat response information for participating firms in general.
- As a wholly private entity, funded by members only and not accepting public funds, the ISAO would serve as a trusted intermediary between the private sector on the one hand and State and federal law enforcement, DHS, and other governmental entities on the other.
- By design, the ISAO would adopt a swarming, team-of-teams approach among the membership to identify threats, share IOCs and TTPs in order to manage threats and to advance other interests of the membership.

Second, the vision is for the ISAO to develop into a cyber workforce development hub for the State. Specifically, the ISAO would engender deeper relationships between its private sector membership and one or more colleges and universities that would result in:

- Shared training facilities on a university campus developed in concert by the ISAO and the university partner. (At ACTRA, equipment establishing a cyber training lab was donated by corporate members with a university partner providing space for the equipment *pro bono.)*
- Student internships at the ISAO command center that would provide skill-enhancing opportunities for undergraduate and graduate students benefitting the ISAO, better preparing students for work roles in the private or public sectors, and exposing companies to these students for possible recruitment
- Collaboration on cybersecurity curricula by using the hub to host a corporate consultative group ala the talent pipeline management program of the US Chamber of Commerce
- Participation in training exercises for members with State and federal entities.
- Establishing or joining a cyber range to serve both corporate and student training

Third, as an informal byproduct of its operation and activities, i.e. through its member meetings at the C-suite level and by bringing together cybersecurity employees from different companies across CI and non-CI sectors in training programs, the ISAO would engender and reinforce trust relationships among the members.

ACTRA. He has serves as a member of the Arizona Threat Intelligence Center (ACTIC) and on the Arizona Cybersecurity Team (ACT) established by executive order and advisory to the Arizona governor.

In all of these ways, the vision is for the ISAO is to replicate the organization, services, and benefits that after seven years of operation ACTRA is able to offer its members.[101]

V. Strategy for Start-up and Longer-Term Operations

In the discussions with ACTRA representatives in Phoenix, three options were offered to help a charter group of Maryland firms launch an ISAO:

- Option 1: Acting as an informal sounding board for Maryland-led efforts.
- Option 2: Engaging ACTRA at a negotiated government rate to assist in planning and organizing a Maryland ISAO.
- Option 3: The "rapid execution/dual membership model" under which the chartering Maryland members aim to become an independent ISAO and peer of ACTRA. Under this option,
    - The chartering members would have dual membership with ACTRA and the Maryland ISAO in CY 2021. The ACTRA membership fee ($6, 500) would be represent a steep discount off the normal member rate.
    - The membership would carry all the benefits enjoyed by ACTRA members and permit visibility into ACTRA's culture, operations backroom support, and range of workforce development programs, including its relationships with K20 education.
    - ACTRA would share key operating documents *pro bono* for adaptation and use under a perpetual IP license.
    - Finally, if the Maryland ISAO needs direct facilitation, ACTRA would be willing to provide consulting support or act as a sounding board at a low contract rate.

This proposal is based on *Option 3* which offers several key advantages:

- It allows for an *immediate value proposition* in CY 2021 for the charter members of the Maryland ISAO through actionable information sharing and participation in the full range of ACTRA programs.
- The Maryland ISAO would be able focus in CY 2021 on membership building and in preparing to become operationally independently as a peer of ACTRA in CY 2022.
- The chartering group would be able to take what they absorb from ACTRA in CY 2021 and adapt it the Maryland ISAO.
- It reduces the effort needed to stand up a Maryland ISAO by taking advantage of ACTRA's willingness to share *pro bono* of legal, governance, and other operational documents to be adapted to Maryland and to serve when needed as a formal consultant at a low rate.

[101] See Appendix I of this document for a more detailed discussion of ACTRA from Cohen and Nussbaum, opus cit.

VI. Legal Form, Governance, Participation Agreement

The Maryland ISAO would be set up as a 501(c)(3) or a 501(c)(6) consistent with the principle of being a grass-roots, industry-created, industry-led, member-funded threat sharing and analysis organization.[102] This would not preclude relationships with State and federal agencies.

It is envisioned that representatives of the organizations chartering the Maryland ISAO would comprise the initial board of directors. Initial board committees likely would include governance, technical operations, and finance for starters with formal committees around new member recruitment, workforce development, and perhaps others to come later. In general, the board of directors would function in a manner consistent with State and federal law and the best practices recommended by the Council of Nonprofits or similar organizations.

Critical to the trust relationship among member organizations is the partnership agreement. This agreement would address at least the following elements:[103]

- Confidentiality, safeguarding and permitted uses of sensitive information
- Rights of ownership and intellectual property rights of sensitive information and derivative works
- Background check requirements
- Non-solicitation of employees

ACTRA is willing to provide *pro bono* its own charter and bylaws as examples for the Maryland ISAO to adapt to its needs.

VII. Notional Participation Fees and Cost Projection

The initial costs to the charter group of six firms might be follows:

Cost per Charter Firm	CY 2021	CY 2022
ACTRA Membership	$6,500	
MD ISAO Support	$40,000	$40,000
Total Cost/Charter Firm	$46,500	$40,000

Through CY 2022, it is assumed that additional firms would be recruited to join the Maryland ISAO. This might call for an articulated membership schedule that the ISAO board and its President/CEO would establish.[104]

Below is a notional cost projection for the start-up based on the proposed relationship with ACTRA outlined above (Section V, Option 3).

---

[102] For a discussion of 501(3)(c) and 501(6)(c) legal form in this context, see ISAO SP 1000, accessed at https://www.isao.org/storage/2017/09/ISAO-SP-1000-Forming-a-Tax-Exempt-Entity-v-1-0.pdf. The requirements for establishing a 501 (c)(3) in Maryland are identified by the Secretary of State's office at https://sos.maryland.gov/Charity/Pages/Non-Profit-Organization.aspx

[103] Bakis and Wang, *opus cit*, p. 22.

[104] See an example fee schedule at *Ibid*, p. 25.

Budget Line Items	**2021**	**2022**	**2023**
Revenues[105]			
ISAO Membership	$240,000	$240,000+	$240,000+
Total	**$240,000**	**$240,000+**	**$240,000+**
Costs			
Executive Director[106]			
Salary	$150,000	$155,000	$160,000
Benefits (30% of salary)[107]	$45,000	$46,500	$48,000
Subtotal – Exec Dir	**$195,000**	**$201,500**	**$208,000**
Travel			
Conferences, meetings	$25,000	$25,000	$25,000
Subtotal - Travel	**$25,000**	**$25,000**	**$25,000**
Office space, equipment, communications support[108]			
Subtotal - Office	**$00**	**$00**	**$00**
Threat-sharing platform and other technologies	**$00**	TBD	TBD
Subtotal - ACTRA	**$00**	TBD	TBD
Total – All Expenses	**$220,000**	**$226,500 +**	**$233,000 +**
Net Revenue	**$25,000**	**TBD**	**TBD**

[105] As noted in the narrative, the assumption is that each of six charter firms would contribute $40,000 in each of CY 2021 and CY 2022 toward the Maryland ISAO itself. Membership expansion is assumed during CY 2023 and succeeding years resulting in a revenue greater than $240,000 for CY 2023 onward.

[106] See Appendix A for position description

[107] This percentage estimate for benefits is based on recent private sector data. *See Employer Costs for Employee Compensation*, Bureau of Labor Statistics News Release, December 18, 2019, Table 4 (Management and professional), accessed at https://www.bls.gov/news.release/pdf/ecec.pdf

[108] The assumption is that office space is donated or that the President/CEO works from home. This follows a model that aims for an organization that has a largely invisible footprint as part of its security culture.

Notional Implementation Plan

Notional Rapid Deployment Timeline

CY 2021		
Month	Goals	ACTRA Support
July - September	Core private sector group is recruited as the founding dues-paying members committed to standing up the ISAO.	ACTRA President/CEO is willing to participate in orientation session to provide more information about ACTRA and to answer questions of the chartering Maryland group.
	Tasks of founding group: a. Decide whether ISAO should be a c3 or c6 organization & organize formally b. Recruit and appoint ISAO President/CEO c. Secure office space (either paid or pro bono) d. Take other decisions as needed	ACTRA will provide *pro bono* the organizational documents that the chartering group can adapt to Maryland
CY 2021		
Month	Goals	ACTRA Support
October - December	a. Maryland ISAO President/CEO in place triggers formal onboarding of Maryland charter group as full ACTRA members for CY 2021 b. Maryland ISAO President/CEO focuses on stakeholder relations and building the membership base and the financial resources of the ISAO c. With a view of becoming an independent entity, the President/CEO secures a threat intelligence sharing platform for the ISAO and in general operationalizes systems, distribution lists, communications structure, etc. d. Buildout of Maryland ISAO as cyber workforce development hub 1. Recruit university partner(s) into the membership to work with private firms to host the equipment for a cyber range and to provide space for a cyber lab for training by students and corporate employees 2. Develop a formal 'Cyber Academy' for corporate members, training for which would occur in the university cyber lab 3. Develop K12 outreach program for offering cyber-related classes for K12 teachers and students	For CY 2021, ACTRA will provide charter members with full ACTRA membership benefits on the same terms as ACTRA members. Exception would be discounted dues of $6,500/year for CY 2021. ACTRA will provide *pro bono* (except for direct costs) operational documents and framework that the Maryland ISAO can adapt as it moves to a fully independent peer ISAO. These documents and framework would be provided gratis under a perpetual IP license. ACTRA available for consulting at a negotiated government rate to help with build out of management and operational systems

CY 2022		
January	Maryland ISAO begins its second year with broader membership, sufficient finances, and systems in place to stand as an independent ISAO in a peer relationship with ACTRA. At this point, the Maryland ISAO is providing not only actionable threat-sharing services but has launched itself as a cyber workforce development hub, offering a range of cyber workforce development programs in Maryland, including corporate training, student internship opportunities, and training aimed at K12 students and teachers	

ISAO APPENDIX A

POSITION DESCRIPTION[109]
PRESIDENT/CEO
MARYLAND ISAO

Duties/responsibilities:

- Would serve as the chief administrative officer for the Maryland ISAO
- Would recruit new members to the Maryland ISAO and manage stakeholder relations
- Would serve as Maryland ISAO liaison to the Arizona Cyber Threat and Response Alliance (ACTRA) and to State and federal law enforcement and other agencies
- Would facilitate integration of new members into the ACTRA threat-sharing platform
- Would work with ACTRA to provide insight into the specific cybersecurity analytic processes and TTPs for Maryland and ACTRA members
- Would provide timely briefs and other reports to the Board of Directors
- Would assist in identifying roles, jobs, tasks, or skills needed in the Maryland ISAO as the organization matured.
- Other duties as relevant

Qualifications

The President/CEO should have a demonstrated track record of building an organization's membership and effectively managing stakeholder relations. Applicants should have a sensitivity to, and understanding of, the unique cultures of the private sector, public sector, academia, law enforcement and intelligence agencies, and demonstrate an ability to see commonality among these key stakeholders versus the differences among them. Crucial are critical thinking and problem solving. Exceptional communications skills to large groups and individually are essential. Applicants should have expertise in cyber defense, incident response, and forensics and be knowledgeable about technologies necessary to the functioning of an ISAO. Highly desirable is some experience with cyber workforce development.

[109] Adaptation of the executive director position description in ISAO 600-1, opus cit., p 16.

ISAO APPENDIX B

LEGAL PROTECTIONS FOR INFORMATION SHARING[110]

TO: Professor Rauschecker, Center for Health and Homeland Security, Francis Carey King Carey School of Law, University of Maryland, Baltimore
FROM: Kevyn Jorgenson, Emma Eiden, Nicky Arenberg, Benita David-Akoro, and Sharon Sidhu
DATE: March 25, 2020
RE: Legal Authority Governing Info. Sharing Networks and Liability Protection

---

Brief Answer and Introduction

The bulk of legal authority, relating to liability protection information sharing networks, can be found within Title I of the Cybersecurity Information Sharing Act of 2015 (CISA or the Act). Title I of CISA outlines various federal rules that govern cybersecurity information sharing and provides for various protections allotted in the course of monitoring, sharing, or receiving cybersecurity information. These protections include protections from liability, non-waiver of privilege, and protections from FOIA disclosure, although, importantly, some of these protections apply only when sharing information with specific types of entities. The key provisions under CISA, which provide the bulk of authority for the transmission of cybersecurity information, are found in Section 103, up through Section 106.

Title I of CISA mainly discusses, and authorizes, provisions relating to "cyber threat indicators" and "defensive measures," as they effect a given information system.[111] A cyber threat indicator, as it used in the context of CISA, is essentially any information that is either necessary to identify, or is directly related to, cybersecurity threats. Cybersecurity threats generally refer to actions that are not protected under the First Amendment, that seek to gain unauthorized access, or cause the disclosure of, an information system, as well as other actions that may otherwise have an adverse effect on the integrity of an information system. Section 102(5)(A).[112] Defensive measures, as it used in the context of CISA, relates to any measures taken to combat

---

[110] Note: This section Is not offered as legal advice.

[111] An "information system" is defined by Section 102 as having the same meaning as is provided under Title 44, Section 3502, of the United States Code. Title 44 of the United States Code houses federal regulations relating to "public printing and documents." The definition provided for an "information system," under Section 3502, was defined as part of Subchapter I of Chapter 35, outlining the federal information policy. Section 3502 defines an information system to mean "a discrete set of information resources organized for the collection, processing, maintenance, use sharing, dissemination, or disposition of information." *See* 44 U.S.C.A. § 3502(8).

[112] Specifically, Section 102 defines a "cyber threat indicator" to mean necessary information that is required to identify or describe: malicious reconnaissance; a method of overriding a security control or exploitation of a vulnerability in security; a security vulnerability; a method used to compel an individual, with legitimate access to an information system, to inadvertently enable the breach of a security control or enable the exploitation of a security vulnerability; malicious cyber command control; the actual or potential harm caused by an incident relating to a cybersecurity threat; any other attribute relating to a cybersecurity threat; and any combination thereof. Section 102(6).

cybersecurity threats, including an action, device, procedure, signature, technique, etc. Section 102(7).

Relevant Requirements and Policies under Title I of CISA

Beginning with Section 103, CISA requires the Director of National Intelligence (DNI) and the Departments of Homeland Security (DHS) and Defense (DOD), and Justice (DOJ) to develop and promulgate procedures that promote the sharing of information relating to cybersecurity threats. The regulation generally requires that these procedures facilitate and promote the federal government's sharing of information pertaining to cyber threats, cyber threat indicators, and cybersecurity best practices with other entities. While the regulation goes on to list some requirements as guidance in developing the procedures, the regulation does not offer extensive, or explicit, requirements of the procedures to be developed under Section 103(a), granting the relevant federal authorities much discretion in their drafting of the guidelines.

While the guidelines do provide the pertinent provisions that govern the sharing of information, CISA does provide explicit authorities and protections from liability within the statutory text. Section 104(c) allows for an entity to share with, or receive from, a cyber threat indicator or defensive measure from any other entity or the federal government, so long as it serves a cybersecurity purpose and is consistent with the protections governing confidential information. The provision explicitly requires that any entity participating in this sharing of information take steps to protect against the unauthorized access or use of that information, by means of developing and implementing security controls and reviewing cyber threat indicators for personal information prior to sharing. The Children's Online Privacy Protection Act further requires the removal of certain information relating to children, such as protected health information, financial information, consumer information, HR information, educational history information. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505.

CISA also requires that any information shared by an entity with the federal government be deemed voluntarily shared information and exempt from disclosure and withheld from the public under any laws of such jurisdictions requiring disclosure of information or records. However, CISA does prohibit DHS from developing a process of sharing information that limits the lawful disclosure of communications, records, or other information relating to known suspected criminal activity, voluntary or legally compelled participation in a Federal investigation, and the sharing of cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement. Section 105(c)(E).

Exemptions and Liability Protections under Title I of CISA

Antitrust Laws

The CISA provisions allow for a specific exemption from liability for entities sharing information, which may otherwise implicate violations of antitrust laws. Antitrust laws concerning the sharing of information and the competition issues that may arise from such

activity is generally governed by Antitrust Guidelines published by the DOJ,[113] business review letters authorized under 28 C.F.R. § 50.6, and Federal Trade Commission advisory opinions.[114] The analytical framework, mapped out by these authorities, generally convey the need for regulation over the exchange of competitively sensitive information due to concerns of potential competitive coordination amongst competitors.

Section 104 grants an exemption for private entities that wish to share information, for cybersecurity purposes, from antitrust laws. The provision explains that "it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title." The Act does, however, limit this exemption as inapplicable to price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning. The DOJ and FTC collaboratively provided a set of guidelines to refer to when analyzing information sharing amongst competitors, which serves as a useful tool for private entities to assess their actions and potential liability implications, as well.[115]

General Liability Protections

Most protections against potential liability resulting from the monitoring, sharing, or receipt of information are also granted under Section 106 of CISA. Provided that the sharing is otherwise conducted in accordance with the Act, sharing conducted through the DHS process will sufficiently trigger the liability protections authorized by Section 106(b). Liability protection also extends to sharing of information with other federal entities when the threat indicator or defensive measure was already shared with DHS through the appropriate mechanism and then the information is shared with another federal entity. Section 105(c)(1)(B)(i).

Similarly, under Section 104(c), non-federal entities may also share cyber threat indicators and defensive measures with federal entities through Information Sharing and Analysis Centers

[113] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS (2000), available at http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf [hereinafter COMPETITOR COLLABORATION GUIDELINES]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTHCARE (1996), available at http://www.justice.gov/atr/public/guidelines/0000.htm [hereinafter HEALTHCARE STATEMENTS]; U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY 13 (1995), available at http://www.justice.gov/atr/public/guidelines/0558.htm [hereinafter IP LICENSING GUIDELINES].

[114] The Federal Trade Commission is granted authority, in certain circumstances, to offer industry guidance in the form of an advisory opinion. *See* 16 C.F.R. §§ 1.1-1.4; *see also* http://www.ftc.gov/tips-advice/competition-guidance/competition-advisory-opinions.

[115] U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS (2000), available at http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf

(ISACs) or Information Sharing and Analysis Organizations (ISAOs), which may share them with federal entities through DHS on their behalf.
In general, ISACs and ISAOs are considered private entities and are thus granted certain protections from liability under Section 106. Section 106(b)(1) provides that private entities that share a cyber threat indicator or defensive measure with ISAC or ISAO in accordance with the Act receive liability protection and other protections and exemptions for such sharing. Section 105(c)(1)(B)(ii) also applies to private entities and grants liability protection for the sharing of information by a regulated private entity with its regulating federal agency, regardless of whether the information is shared through the DHS' channels.

Liability Protections for Sharing Information with ISAOs

The Information Sharing and Analysis Organization Standards Organization (ISAO SO) is a non-governmental organization that was created to facilitate the implementation of Presidential Executive Order 13636.[116] Upon the organization's establishment, the ISAO SO drafted numerous publications to serve as guidelines for entities and governmental bodies to refer to when faced with issues of liability protections.

The DHS guidelines, and ISAO SO guidance documents take a similar approach in establishing liability protections that exist when issues arise due to liability for sharing information with ISAOs. Both the DHS guidelines and ISAO SO publications rely on the liability protections established within Section 106 of CISA. Additionally, the ISAO SO guidance documents identify the "SAFETY Act"[117] as a possible source of liability protection for providers of Qualified Anti-Terrorism Technologies.

ACTRA Approach in Seeking Liability Protections

While there are clear and expansive protections authorized under CISA, with regard to liability protection implicated by the sharing of information, technical, political, and legal issues are bound to arise when different types of entities with different or even competing interests culminate to exchange information in a formal setting. However, an organization in Arizona was created for this purpose, and serves as a case study for information sharing between private and public entities.

[116] Executive Order 13636 of February 12, 2013, entitled "*Improving Critical Infrastructure Cybersecurity*," was issued in response to threats facing the Nation's critical infrastructure due to potential cyber attacks. EO 13636 directed Executive Branch to lead these efforts by means such as developing cybersecurity frameworks that were technology neutral and voluntary, increasing the amount of information sharing regarding cyber threats, incorporating privacy and civil liberties protections into the initiatives led under the Order, and exploring the use of existing policy and regulation to promote cybersecurity and protection of the Nation's critical infrastructure.

[117] The "Support Anti-Terrorism by Fostering Effective Technologies Act of 2002," or the "SAFETY Act," was enacted as Subtitle G of Title VIII of the Homeland Security Act of 2002 and creates federal cause of action for claims against providers of qualified anti-terrorism technology where that technology was used to protect against, in response to, or for recovery purposes after an act of terrorism. 6 U.S.C. ¢ 44(a).

The Arizona Cyber Threat Response Alliance, Inc. ("ACTRA") is a non-profit corporation that facilitates the sharing of information between different groups and entities with the goal of improving the Nation's response to cyber security events.[118] The organization was undertaken by the private sector with the active involvement of the FBI, DHS, and Arizona Counter Terrorism Information Center ("ACTIC"). Ultimately, ACTRA was created "to serve as the self-governed private sector-controlled hub for cyber information exchange and response."[119]

As part of their strategy in facilitating information, ACTRA sought to promote information sharing and trust-based communication between private and public sectors by creating a buffer between government agencies and private sector companies. As part of membership to ACTRA, all members are required to sign a non-disclosure agreement. Furthermore, the organization provides that all meetings are governed by "Chatham House Rules."[120] These legal requirements and standards in place prevent members of ACTRA from discussing any details about ACTRA or its members' companies and organizations without having explicit consent to do so.

Members of ACTRA attend monthly briefings facilitated by the FBI and DHS agencies for unclassified information sharing and are open to all members and key agency stakeholders. Briefings for classified information are held quarterly. These briefings are cited as "essential to developing a working relationship and inter-reliance between private and public-sector individuals and cyber professionals, and agency stakeholders within the state of Arizona." [121]

The actual platforms in which information is shared is owned by the member organizations themselves, which similarly provides members with a greater confidence in the anonymity of the information sharing fostered by ACTRA. As part of ACTRA's information sharing model, the organization places a strong emphasis upon the quality and value of the intelligence that is shared, and thus suggests that all intelligence shared amongst members be limited to new or unusual tactics, techniques, and procedures (TTPs), and/or vulnerabilities.[122]

---

[118] *See generally* https://azinfragard.org/actra/

[119] *See Id*.

[120] *See https://www.newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/appendix-ii-arizona-and-the-arizona-cyber-threat-response-alliance-actra-the-community-approach/* (Under Appendix II: Arizona and the Arizona Cyber Threat Response Alliance (ACTRA): The Community Approach"); *see also* https://www.chathamhouse.org/chatham-house-rule.

[121] *Id*. *Citing* 25 Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Office. (N. Cohen, Interviewer).

[122] *Id*. *Citing 24 Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer); ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer*) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.

ISAO APPENDIX C

ACTRA CASE STUDY:

THE ARIZONA CYBER THREAT AND RESPONSE CENTER (ACTRA)
(From Cohen and Nussbaum, Cybersecurity for the States: Lessons from Across America, New America, May 2018, Appendix I)

Overview

To tackle the cybersecurity challenges facing the state, Arizona has created a "team of teams."[16] One of these teams, the Arizona Cyber Threat Response Alliance (ACTRA), is an Information Sharing and Analysis Organization (ISAO) formed in 2013. Its stated mission is to serve as the "hub for collaborative cyber information sharing in a neutral environment of trust where partners from industry, academia, law enforcement and intelligence come together, leveraging cross-sector resources to more effectively analyze critical, real time intelligence and respond to emerging cyber threats to Arizona's Critical Infrastructure and Key Resources."[17]

ACTRA has its roots in the Arizona InfraGard[18] and remains wholly independent of, but closely aligned to that organization as its "operational cyber arm" by agreement. In 2012, the AZ InfraGard initiated a planning effort, led by current ACTRA CEO Frank Grimmelmann, to understand and respond to barriers to effective bi-directional communication and information sharing between private and public sector organizations. Although this effort was led by members of the private sector, there was active involvement from the local Federal Bureau of Investigation (FBI) and U.S. Department of Homeland Security (DHS) offices and the Arizona Counter Terrorism Information Center (ACTIC). The study found a need for a separate but affiliated non-profit entity that could serve as the "self- governed private sector-controlled hub for cyber information exchange and response."[19]

This arrangement allows ACTRA to focus only on cybersecurity information sharing and communication needs, and creates an effective, independent conduit (or buffer) between its private sector and public sector Member Organizations, and the agencies nationally. This separation engenders trust in the anonymization of data shared with government agencies and helps to coordinate the efficient flow of communication. Rather than place the burden on public sector agencies to choose which private sector entities to inform and involve in specific cybersecurity efforts, ACTRA serves as the point of contact for its private and public sector Members, engaging the various members as needed. Its affiliation with InfraGard—all direct member touchpoints of ACTRA must also be InfraGard members—allows ACTRA to pre-vet its members without additional expenditure of resources.

Representatives from ACTRA sit in the ACTIC, Arizona's "all-hazards" Fusion Center that serves as Arizona's analytic and dissemination organization statewide. ACTRA's president also sits on the ACTIC's executive board representing private sector, as a bridge to law enforcement and intelligence. The Fusion Center processes various threat and information feeds and

communicates critical information to state/local/tribal entities, critical infrastructure operators, and nontraditional organizations. Structurally, the ACTIC sits within Arizona's Department of Homeland Security, although the chief information security officer for the state reports directly to the Arizona CIO, who resides in the Arizona Department of Administration.

Arizona also runs several other initiatives, some of which are run in concert with or are supported by ACTRA. These include various exercises that span across the private and public sectors, including federal and state partners, including regional cybersecurity workshops that reached over 750 people in the latter half of 2017, mostly in underserved areas. The State CISO and the ACTRA's CEO, Frank Grimmelmann, co-chair the new Arizona Cybersecurity Team (ACT), an executive level initiative launched in 2018 by Governor Doug Ducey to coordinate the various groups around Arizona working on cyber issues. The ACT includes representatives from federal, state (legislative and executive branches), and local government, the private sector, and higher education.[20] These members represent the various groups with a stake in cybersecurity in the state; given Arizona's established strategy of working through a team of teams, this organization will help to formalize this structure.

The following section describes the successes and challenges of having strong private sector leadership and widespread involvement in a state's cybersecurity program, and the factors that have enabled this model to flourish in Arizona.

Successes

Information Sharing

Fusing Member Organization policymakers, legal representatives, and technical professionals, ACTRA's information sharing initiatives are diverse and highly dependent on the culture of trust established throughout the organization and its members. This sense of assurance is established first at the personal level, and subsequently empowers organizational dealings at every level. All ACTRA members sign an NDA, which prevents them from discussing any details about ACTRA or its member companies without explicit permission to do so. "Chatham House Rules" are also mandated for every ACTRA event. Because the information shared and the platform on which data is shared are owned by the member organizations themselves, members don't feel as though they are communicating directly with a U.S. government agency, and have greater confidence in the anonymization of the information sharing.[21] If the government needs or desires to identify the originator of the intelligence, they can route the request through ACTRA.[22]

The need to share and deliver accurate information is manifested in efforts to align the self-interest of all key stakeholders and drives ACTRA's National Security/Risk Management Value Proposition. ACTRA's goal is to "deliver a timely, cost effective, actionable individual and/or collective response to protect individual critical sector corporate assets, and improve our national security through adopting a unique collaborative structure."[23] In order to do so, ACTRA and its members place a heavy emphasis on the quality and value of the intelligence it shares. For its direct or manual information sharing mechanisms, ACTRA strongly suggests that intelligence

shared be limited to *new* or unusual tactics, techniques, and procedures (TTPs), and/or vulnerabilities.[24]

Specific information sharing initiatives include email alerts sent directly by members to other vetted member touchpoints, specialized sharing per industry (e.g. supplier threats to an industry), disseminating information via a shared threat intelligence system that includes STIX/TAXII feeds and a plug-in for most SIEM platforms, and both unclassified and classified ACTRA FBI Tear Sheet Exchanges held at the Arizona Fusion Center, that include FBI and other agency briefs. The latter briefings, facilitated by the FBI and DHS agencies, are held monthly (classified briefings being held quarterly,) and are open to all members and key agency stakeholders under Chatham House Rules and legal protection.

The briefings are essential to developing a working relationship and inter- reliance between private and public-sector individuals and cyber professionals, and agency stakeholders within the state of Arizona. If the government stakeholders share real actionable information, private institutions are more likely to share information back. The discussions that stem from these briefings are also useful both for the private sector representatives in attendance and for the government briefers, as they often go further into detail and impact than a one-directional briefing could achieve.[25] Regular C-suite Level roundtables coordinated by Arizona's CISO Mike Lettman also aid in this ongoing effort.

The Threat Unit Fellow (TU F) Program

ACTRA's information sharing efforts are facilitated by the Threat Unit Fellow (TUF) Program. The ACTRA Cybersecurity Academy (ACA) runs a 300-hour apprenticeship/training program with a robust cyber threat analysis curriculum, and real-world experience across all ACTRA organizations. Upon graduation from this program, TUF members become a part of the ACTRA Virtual SME[26] Response TUFTeam (VSRT) and serve as analysts in ACTRA and at their own organizations, where they can feed information to the Threat Intelligence Platform and provide a virtual watch center service. This is further complemented by a physical Watch Center that triages incidents among VSRT TUFTeam members.

These physical ACTRA trained TUFTeam VSRT members are employed by an MSP stakeholder, and have dedicated hours and bifurcated systems so that they can monitor the ACTRA systems and their own client systems simultaneously. However, ACTRA information is fed only back to those customers who are members of ACTRA.[27] Additionally, ACTRA distributes formal non-attributed advisories as requests for information (RFI) across the InfraGard and ACTIC networks. By exception approved by a Member Organizations, these can be shared with attribution with these external networks or a subset of them under the control of the member.

The TUFTeam Training is available to ACTRA Member professionals across the private and public sector and serves to build relationships between individual organizations and across sectors. Thus far, private sector, state, federal and local analysts have gone through the training; law enforcement officials and National Guard service members are scheduled to attend a session in the second quarter of 2018, while keeping the lanes in the road separate to align diverse stakeholder's self-interests.

Workforce Development

In addition to the TUFTeam/VSRT programs, ACTRA has several collaborative volunteer-driven Cyber Warfare Ranges "in the wild" for community leveraging community outreach and workforce development. One range is physically located at Grand Canyon University (but not a university resource), and the second range is located in the City of Mesa's Arizona Labs also operating independently through an identical structure. These ranges "enable penalty-free offensive and defensive exercises, and real-world operations that provide knowledge and forensic insight into how to better defend infrastructure by getting into the head of the adversary."[28] They also enable security professionals to test defensive infrastructure without risking actual organizational data.[29]

These collaborative endeavors also serve as a training ground for any individuals who may want to gain practical expertise in the field. A headhunter volunteers at the range to help place individuals who have gained experience on the range with companies needing security professionals.[30] Volunteers at the ranges are working on curriculum sets that would institutionalize some of the training elements and make it more aligned with prospective employers.

ACTRA and its members also work with the Phoenix Chamber of Commerce, which has a cyber workforce collaborative initiative directed by Jennifer Mellor. One initiative, which utilizes the SkillBridge[31] and Career Skills Program (CSP),[32] both offered by the U.S. Department of Defense, provides government sponsored six-month apprenticeships in public and private organizations for service members leaving the military.

Once that period is completed, companies who take part in the program providing internships can then hire the trained individual at their own discretion. This program was discovered by an ACTRA member company as part of their relationship with southern Arizona military facilities and has now expanded as a pilot to other members and to other military installations in Arizona.[33] In turn, ACTRA just announced that the program will be rolled out across all of Arizona shortly through a rapid deployment methodology developed during the ACTRA pilot in cooperation with the ACTRA Member Organization serving as the Team Lead.

Cyber Defense

ACTRA is written directly into the Cyber Annex to Arizona's emergency response plan.[34] Per this plan, in the case of an incident, ACTRA is tasked along with bidirectional communications to:

- provide resources to the Arizona Department of Administration and all Arizona state government agencies upon request;
- assist the FBI with managing and facilitate the state's role in critical infrastructure protection; and
- communicate and report information on observed cyber security incidents.

Since its inception, ACTRA has yet to be called upon for such a coordinated incident response, but after news broke about Russian targeting of the Arizona election system in 2016[35], state officials received offers for aid from several members of ACTRA.[36] ACTIC and ACTRA have also held multiple exercises to coordinate efforts in the case of an incident.[37] Additionally, ACTRA VSRT Members have been stood up alongside agencies in the Multi-Agency Coordination Center (MACC) during a major event and expect to during other major Arizona events in the future.

ACTRA also facilitates participation in regional and national table top and live exercises run by DHS, DoD, and other organizations.[38] Representatives from public and private member organizations regularly participate in these exercises, which further increases the personal ties in the cyber ecosystem and provides exposure to national efforts and related activities performed in other areas of the country.[39]

ACTRA has three additional programs designed to increase the capabilities of cyber defense within its purview. The first such program is the ACTRA Think Tank, an invitation-only brain trust of experts who can translate the challenges experienced by members and threats observed on the ranges to solutions for the market. The think tanks drill down into particular issues and sometimes uses a member organization's infrastructure (with member approval) to test solutions.

The ACTRA Special Operations Group then operationalizes those findings. These two teams have made progress in efforts to increase reliable automation by connecting various SIEM platforms with ACTRA's Threat Intelligence system, and to leverage resources in the development of additional solutions available across ACTRA.

The third program is channeled through a local university and enables students to perform open source cyber intelligence collection. In large part because of ACTRA's imprimatur (or engagement), the Phoenix FBI, DHS and other agency stakeholders supports the program, and agency stakeholders provide briefings to the students on how to remain legal in their activities.[40] With its deep network, ACTRA also serves as a point of contact for technology transfer programs within universities and chosen vendor stakeholders, when they might be looking for potential pilot sites or feedback on new cyber technologies.[41]

Notes to ACTRA Case Study

16. Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer)
17. Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8
18. InfraGard is a partnership between the FBI and members of the private sector. The InfraGard program provides a vehicle for public-private collaboration with government to expedite the timely exchange of information and promotes mutual learning opportunities relevant to the protection of Critical Infrastructure.
19. Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8
20. Governor Ducey Announces Appointments to Arizona Cybersecurity Team. (2018, 3 7). Retrieved from Office of the Governor Doug Ducey: https://azgovernor.gov/governor/news/2018/03/governorducey-announces-appointments-arizonacybersecurity-team
21. Figueroa, C. (2018, 1 19). Protective Security Advisor for Arizona, Department of Homeland Security. (N. Cohen, Interviewer)
22. ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)
23. Arizona InfraGard. (2018, 3 25). Arizona Cyber Threat Response Alliance. Retrieved from Arizona InfraGard: http://azinfragard.org/?page_id=8
24. Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer); ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.
25. Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Once. (N. Cohen, Interviewer)
26. Subject Matter Expert
27. ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.
28. Grimmelmann, F., Halla, D., & Nix, M. (2016). A Development Guide for Regionally Based Information Sharing and Analysis Organizations. Laurel, MD: Johns Hopkins Applied Physics Laboratory.
29. ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.
newamerica.org/cybersecurity-initiative/reports/cybersecurity-states-lessons-across-america/ 53
30. Halla, D. (2017, 12 7). Senior Advisor, Johns Hopkins Applied Physics Laboratory. (N. Cohen, Interviewer)
31. DoD SkillBridge: https://dodskillbridge.com/
32. U.S. Army Installation Management Command. (2017, 7 12). Army Career Skills Program. Retrieved from Stand-To!: https://www.army.mil/standto/2017-07-13

33. ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer); Mellor, J. (2018, 1 18). Vice President of Economic Development, Phoenix Chamber of Commerce. (N. Cohen, Interviewer)
34. Arizona State Emergency Response and Recovery Plan. (2016, 9 1). Retrieved from Arizona Department of Emergency Management: https://dema.az.gov/sites/default/les/publications/EMPLN_State_Emergency_Response_and_Recovery_Plan-Basic_Plan_SERRP_2016FINAL_Oct7.pdf
35. Nakashima, E. (2016, 8 29). Russian hackers said to have targeted Arizona election system. Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-electionsystems/2016/08/29/6e758□4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.743ef514efce
36. ACTRA Member Interviews. (2018, 1 18 & 19). (N. Cohen, Interviewer) Note: Because ACTRA members are under NDA they cannot be cited specifically. The author spoke with 14 individual ACTRA members from both the public and private sectors.
37. ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)
38. ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)
39. ACTRA Member Roundtable. (2018, 1 19). (N. Cohen, Interviewer)
40. Grimmelmann, F. (2018, 1 Multiple Interviews). CEO, ACTRA. (N. Cohen, Interviewer); Hellmer, M. (2018, 1 19). SSA Phoenix Cyber, Phoenix FBI Field Office. (N. Cohen, interviewer)
41. Shakarian, P. (2017, 12 13). Fulton Entrepreneurial Professor, Arizona State University. (N. Cohen, Interviewer)

APPENDIX C

Maryland Cyber Security Council Members by Sector

Maryland Cybersecurity Council

Chair

Brian Frosh
Maryland Attorney General

Legislative Representatives

Senator Katie Fry Hester (District 9)
Senator Susan C. Lee (District 16)
Senator Bryan W. Simonaire (District 31)
Delegate Ned Carey (District 31A)
Delegate MaryAnn Lisanti (District 34A)

State Institutions

Vince Difrancisci, Director, Cybersecurity and Aerospace
Maryland Department of Commerce
Designee for Kelly M. Schulz
Secretary

David Engel
Director
Maryland Coordination and Analysis Center

Major General Timothy E. Gowen
Adjutant General
Maryland Military Department

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

Mark Hubbard
Deputy Director
Governor's Office of Homeland Security
Designee for Walter F. "Pete" Landon

Linda Lamone
Administrator of Elections
State Board of Elections

Michael Leahy
Secretary of Information Technology
Department of Information Technology

Colonel William Pallozzi
Secretary of State Police
Department of State Police

Russell Strickland
Director
Maryland Emergency Management Agency

Cybersecurity Companies

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

James Foster
CEO
ZeroFox

Zuly Gonzalez
Co-Founder and CEO
Lightpoint Security

Terri Jo Hayes
Executive Consultant
Mfusion, Inc.

Miheer Khona
CEO
Rising Sun Advisors

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

Larry Letow
Executive Vice President
Myriddian, LLC

Rajan Natarajan
CEO
QualityPro, Inc.

Jonathan Prutow
Project Manager
eGlobalTech

Business Associations

Don Fry
President and CEO
Greater Baltimore Committee

Brian Levine
Vice President for Technology and Innovation
Tech Council of Maryland
Designee for Marty Rosenberg, CEO

Anthony Lisuzzo
President
Army Alliance

Joe Morales, Esq.
Attorney
Maryland Hispanic Chamber of Commerce

Christine Ross
CEO
Maryland Chamber of Commerce

Gregg Smith
Chairman of the Board
Cybersecurity Association of Maryland

Troy Stoval
CEO/Executive Director
TEDCO

Steven Tiller
Board Member
Fort Meade Alliance

Higher Education

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

Michel Cukier, Ph.D.
Associate Professor and Director, ACES Program
University of Maryland

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 Carey School of Law

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

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

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

Dr. Kevin Kornegay, IoT Security Professor
Cybersecurity Assurance & Policy (CAP) Center Director
Designee for David Wilson, Ed.D.
President, Morgan State University

Crime Victim Representative

Sue Rogan
Director of Financial Education
Maryland CASH Campaign

Susceptible Industries

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

Joseph Haskins Jr.
Chairman, President, and CEO
Harbor Bank
Clay House
Vice President of Architecture, Planning, and Security
CareFirst

Pegeen Townsend
Vice President of Government Affairs
Medstar Health

Federal Institutions

Barry Bosman
Director for State and Local Affairs
National Security Agency

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

Rodney Petersen
Director, National Initiative of Cybersecurity Education
National Institute of Standards and Technology

Other Stakeholders

Robert W. Day Sr.
Councilman
College Park City Council

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

Howard Feldman, Esq.
Partner
Whiteford, Taylor & Preston

Brian Israel
Dixon Hughes Goodman LLP

Mathew Lee
CEO
Fastech

Blair Levin
Nonresident Senior Fellow, Metropolitan Policy Program
Brookings Institution

Jonathan Powell
US Department of the Navy

Paul Tiao, Esq.
Partner
Hunton & Williams, LLP

APPENDIX D

Cybersecurity Workforce Survey
Sponsored by the Cybersecurity Association of Maryland (CAMI)

The 2021 Cybersecurity Workforce Survey

The full summary of the survey results may be found here.

(For questions, please contact marylandcybersecuritycouncil@umgc.edu)