MARYLAND CYBERSECURITY COUNCIL BIENNIAL ACTIVITIES REPORT

JULY 1, 2025

`

TABLE OF CONTENTS

`

Statutory Requirement

This is the fifth biennial activities report of the Maryland Cybersecurity Council covering FYs 2024 and 2025. The report is required by SB 542 (2015). 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.[2]

[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". The draft version of this report was developed by Dr. Greg von Lehmen, University of Maryland Global Campus, as staff to the Maryland Cybersecurity Council.

[2] https://www.umgc.edu/mdcybersecuritycouncil

`

Executive Summary

> *As we move forward, we must also recognize that cybersecurity is not solely the responsibility of the government. It requires a whole-of-society approach, with every individual, organization, and sector playing their part.*[3]

The purpose of the Maryland Cybersecurity Council is to assess the breadth and depth of cybersecurity risk to the State, to make appropriate policy recommendations, and to serve as a reservoir of expertise for informing legislation and regulations. To do these things, the Council was chartered as a stakeholder group with broad representation from State government, critical infrastructure, business, academia, and the nonprofit sectors.

Since the Council's last biennial report, there have been over 1,800 *reported* breaches of public and private organizations in the US.[4] These events have aimed at exfiltrating sensitive information, disrupting normal organizational operations, or have been mixed in their intended impacts. There has been no critical infrastructure sector, whether public or private, that has not experienced an attack aimed at disruption. There are few American adults who have not had sensitive personal information compromised.

Maryland is no stranger to these facts. The last two years have seen ransomware or other attacks impacting its local governments,[5] school districts,[6] and private critical infrastructure.[7] Some of these were direct attacks on Maryland entities. Others were supply chain attacks that resulted from the exploitation of vendor services or interconnected systems among regional or national organizations with entities or infrastructure in Maryland.

---

[3] Securing America's Digital Future (2024). A Report by the McCrary Institute for Cyber and Critical Infrastructure at Auburn University and the Cyberspace Solarium Commission 2.0. https://mccraryinstitute.com/presidential-transition-task-force-report/

[4] See University of Maryland CISSM Cyber-attacks Database. Accessed April 23, 2025. https://gotech.umd.edu/research-impact/publications/cyber-events-database-home

[5] See Sabol, B. (2025, February 24). Anne Arundel County likely experiencing a ransomware attack. WMAR2News. https://www.wmar2news.com/local/anne-arundel-county-likely-experiencing-ransomware-attack and Carignan, S. (2024, May 16). Myersville, MD, struck by cyber attack via email last year. The Frederick News Post. https://www.govtech.com/security/myersville-md-struck-by-cyber-attack-via-email-last-year

[6] See Olaniran, C (2025, April 23). Data breach prompts increased cybersecurity for Baltimore City Public Schools. WJZ News. https://www.cbsnews.com/baltimore/news/baltimore-city-public-schools-cybersecurity-breach-maryland/, Prince George's County Public Schools (2024, February 16). Cyber Notice. https://www.pgcps.org/offices/communications-and-community-engagement/newsroom/news/featured/pgcps-network-outage/february-16-2024-cyber-notice?utm_source=chatgpt.com and Dickstein, R. (2025, January 12). School software hack could expose student, teacher data.WMAR2News. https://www.wmar2news.com/local/school-software-company-hack-could-expose-maryland-student-teacher-data

[7] See Gibson, K (2024, October 8). Water supplier American Water Works says systems hacked. https://www.cbsnews.com/news/security-hack-breach-american-water-works/, Robinson, L. (2024, May 10). St. Agnes Ascension Hospital in Baltimore limits service amid suspected cyber attack. WBAL-TV 11 News. https://www.wbaltv.com/article/st-agnes-ascension-hospital-suspected-cybersecurity-attack/60747684 and Maucione, S (2024, March 8). Maryland Medical Providers Still Assessing Impact of United Healthcare Cyber Attack. https://www.wypr.org/wypr-news/2024-03-08/maryland-medical-providers-still-assessing-impact-of-united-healthcare-cyber-attack and Johnson, Derek (2025, May 21). A house full of open windows: Why telecoms may never purge their networks of Salt Typhoon. Cyberscoop. https://cyberscoop.com/salt-typhoon-chinese-hackers-us-telecom-breach/

`

At the same time, more Maryland residents than ever are being notified of breaches of their sensitive personal information. As required by State law, any data breach implicating certain types of sensitive personal information of a Maryland resident must be reported by the affected entity to the Attorney General's Office. Before 2020, that office received 50-100 breach notifications per month. Since 2020, that number has accelerated to 120 -180 per month. In 2022 alone, the number of residents impacted by these breaches exceeded 940,000.[8] This exposure of personal information certainly contributes to various forms of internet crime. Among states, Maryland's financial losses per 100,000 people ranked 14th and 15th, respectively, in 2023 and 2024.[9]

Cybersecurity Risk & The Council's Activities in the Biennial Period

It is within this context that the Council has focused on cybersecurity risk in three of the four national critical functions (NCFs) defined by the Cybersecurity and Critical Infrastructure Security Agency (CISA): connect, distribute, manage, and supply. Specifically, the Council's engagement has focused on the cybersecurity of electric and public water utilities serving Maryland (distribute), the risks to the State's healthcare ecosystem (manage), the exposure implicit in the State government's legacy IT (manage), the cybersecurity talent gap (supply), and consumer privacy and digital safety (manage). Its engagement has been both with the State legislative and regulatory processes and with public education on cybersecurity issues. These activities were informed by its many meetings (20 during the biennium), invited expert speakers, and the research reports that it was able to commission.

The Council's Connection with Legislation and Regulation

It is primarily members of the General Assembly who give effect to the Council's work by connecting it to the legislative process. In the last biennium, these were Senator Katie Fry Hester (District 9), Senator Sara Love (District 16), Senator Dawn Gile (District 33), Delegate Anne Kaiser (District 14), Delegate Kenneth Kerr (District 3), Delegate Andrea Fletcher Harrison (District 24), and Delegate Catherine Forbes (District 43B). Senator Hester in particular, as a Council member and subcommittee chair since 2019, developed many opportunities for the Council and its staff to contribute to legislation. Apart from this process, for the period of this report, the Maryland Public Service Commission was a similar 'connector' to public policy making by inviting the Council to participate in its 2024 cybersecurity rulemaking proceeding. In exercising these roles. the Council has made policy recommendations, responded to requests for assistance in drafting bills and regulations, participated as invited members on stakeholder and working groups, and testified in hearings.

[8] Comments by Jennifer Donelan, spokesperson for the Attorney General's Office. See Kinsale, Natalie (2024, August 2). Addressing the surge in data breaches: Protecting Maryland residents from identity theft. Legal Eye Investigations LLC. https://www.legaleyeinvestigations.com/post/addressing-the-surge-in-data-breaches-protecting-maryland-residents-from-identity-theft

[9] See FBI Internet Crime Complaint Center (2023). Internet crime report. (p. 29) https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf and FBI Internet Crime Complaint Center (2024). Internet crime report. (p. 23). https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

As detailed below, this means that with respect to the national critical functions, the Council's activity was intertwined with successful legislation that concerned community water service cybersecurity, cyber workforce development, IT modernization addressing the risks of legacy systems, and consumer privacy. The Council also helped inform a bill on the cybersecurity of the healthcare ecosystem that did not become law but began the legislative conversation on a critical issue. With respect to regulation, Council members and staff contributed to the final rules of the Public Service Commission to implement the Critical Infrastructure Act of 2023.

Council and Public Education

Beyond its contributions to legislative and regulatory processes, the Council has engaged in public outreach on cybersecurity issues. As in past years, the Council has organized webinars on topics related to cyber hygiene and consumer online privacy rights. These webinars—three in this biennium—included the participation of the Attorney General's Office and Senator Love. As part of its outreach, the Council also organized a panel at the CyberMaryland conference in December of 2023 for two legislators—Senator Hester and Senator Love—to discuss a range of cybersecurity issues facing the State and its residents before an audience of more than 600 attendees.

Looking Ahead to the Next Two years

With each biennial report, the Council tries to look ahead to issues on which it will focus. As transformative technologies, quantum computing (QC) and artificial intelligence (AI) present new cybersecurity and other closely related risks. Given the trajectory of these technologies, the General Assembly amended the Council's charter in 2025 to name these risks and to ensure that they would be within the scope of the Council to consider. As a result, these risks will constitute a priority for the Council in the biennium ahead. At the time of this writing, this is bracketed only by the uncertainty about whether the federal budget reconciliation bill will preempt this agenda in part.[10]

[10] See Note 57 infra.

`

Maryland Cybersecurity Council Activities Report
2023- 2025

Introduction

Cybersecurity risk is a function of the likelihood of a compromise and the potential impact on the confidentiality, integrity, and availability of data and systems.[11] The Cybersecurity and Critical Infrastructure Security Agency (CISA) aggregates this risk across the four national critical functions—connect, distribute, manage, and supply—to better understand the impact of asset-level attacks on individuals, localities, regions, and the country as a whole.[12] Indicators are that risks have been accelerating nationally in terms of both frequency and cost.[13]

The Council's statutory charge includes both express responsibilities and a broad mandate to consider the many faces of cyber risk to Maryland. As discussed below, those express responsibilities will grow with legislative amendments that will take effect this October.[14] This expansion in the Council's charter is matched by changes in the Council's membership and governance.

The Council's current statute requires it to assess the risk to critical infrastructure in Maryland, assist critical infrastructure entities not covered by Federal Executive Order 13636 to meet federal cybersecurity guidance, and encourage and assist private sector firms to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework. The Council is also charged to identify regulatory inconsistencies between State and federal cybersecurity law that may complicate compliance by Maryland businesses, support the creation of a cybersecurity resiliency plan for the State, and recommend *any other* legislation to address cybersecurity issues.[15] Over the years, the Council has exercised this 'elastic clause' to consider issues pertaining to consumer privacy, the privacy of children online, cyber workforce development, and adult cyber hygiene, among others.

Within this biennium, the Council has focused on five sources of cyber risk within the national critical functions. These are risks related to utilities serving Maryland (water, electricity), healthcare, legacy IT in State government, the talent gap, and consumer privacy and safety.[16] This report reviews the Council's activities in these areas for the last two years and looks ahead

---

[11] Joint Task Force (2018, December). Risk management framework for information systems and organizations. NIST. SP 800-32r2. (Page 104). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[12] CISA (2019). National Critical Functions. https://www.cisa.gov/topics/risk-management/national-critical-functions
[13] Government Accounting Office (n.d.). An overview of cyber challenges facing the nation, and actions needed to address them. https://www.gao.gov/cybersecurity
[14] Ch, 627. Acts of 2025 (SB 294/HB 376). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0294?ys=2025RS
[15] Ch. 358. Acts of 2015 (SB 542). https://mgaleg.maryland.gov/2015RS/chapters_noln/Ch_358_sb0542E.pdf
[16] See Note 2 supra for lists under each national critical function. Utilities fall under "Distribute". The provision of healthcare under "Manage", the operation of State government under "Manage", the talent gap under "Supply" and consumer privacy and safety under "Manage"

to issues it will give particular attention to in the next two. To provide a framework for this discussion, it begins with an overview of the Council itself.

Council Organization and Staffing

By statute, the Council is chaired by the Maryland Attorney General or the Attorney General's designee(s). It includes 45 other members organized into six permanent subcommittees. The membership is a mix of statutorily designated and discretionary seats, with appointments reserved for the Attorney General, the President of the Senate, and the Speaker of the House. Key federal agencies, State departments and agencies, including the Board of Elections, State legislators, and various sectors of the State are represented on the Council: critical infrastructure, higher education, the cybersecurity services sector, small businesses, statewide business and technology associations, and nonprofits. In addition to its appointed members, the Council engages 'contributors', viz. individuals who are not appointed members but who are willing to offer their time, expertise, and perspective.

The Council's design provides it with several advantages in pursuing its statutory charge:

- *Its size and stakeholder diversity enable it to capture a broad array of cybersecurity issues affecting Maryland residents.* The Council is based on the "whole of community" approach to cybersecurity. It includes representatives from the Governor's cabinet, the State Board of Elections, the General Assembly, critical infrastructure, academia, advocacy groups, and the cybersecurity industry, among other sectors.
- *The Council functions as a convener of expertise to inform its recommendations and its other activities*. This role is sometimes exercised through the Council's standing subcommittees and through ad hoc subcommittees and working groups. This expertise comes from the Council membership itself, invited policy experts, and other states willing to share information about their successful initiatives and models. The results have been captured not only in meeting minutes and other documents but in the Council's substantive reports.
- *The inclusion of members of the General Assembly creates a direct bridge between the Council and the legislative process*. The relationship between the Council and its legislative members is a dynamic one. Legislative members have leveraged the Council to explore cybersecurity issues and make use of its reports and recommendations to shape legislation. Council members are willing to contribute their expertise to drafting bills, join stakeholder working groups, and provide supporting testimony in committee. In the process, other legislators apart from the Council are engaged or leverage it in some way. The Council's current legislative members are Senator Katie Fry Hester (District 9) and Senator Bryan Simonaire (District 31). Oher legislators whose bills the Council has supported include Senator Sara Love (District 16), Senator Dawn Gile (District 33), Delegate Anne Kaiser (District 14), Delegate Kenneth Kerr (District 3), Delegate Andrea Fletcher Harrison (District 24), and Delegate Catherine Forbes (District 43B).

As a working body, the Council is organized into six permanent subcommittees, each with a focus on particular issues. The six subcommittees are Law and Policy, Critical Infrastructure, Cybersecurity Education and Workforce Development, Economic Development, State Incident Response, and Public Outreach. The objectives of each subcommittee and their members can be found in Appendix A. In addition to these subcommittees, the Council often convenes ad hoc

working groups, and its members may participate in other meetings organized by the Council's legislative members.

By statute, the University of Maryland Global Campus (UMGC) is the permanent staffing agency for the Maryland Cybersecurity Council. 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.

Council Activities in Detail

Convening Expertise: The Council's Due Diligence

The purpose of the Council's plenary meetings is to hear presentations by subject matter experts on cybersecurity issues, receive updates from its subcommittees on their work, and consider policy recommendations[17] and other initiatives within its charter. During the biennium, it met in plenary session six times. Presenters for this period included:

- Chris Inglis, former National Cyber Director and NSA deputy director ('Critical Infrastructure and the Cybersecurity Threat Landscape')
- Seeyew Mo, Senior Advisor to the CyberMaryland Program, and former White House Assistant National Cyber Director for Cyber Workforce, Education, and Economic Advancement ('Growing Maryland's Cybersecurity Workforce')
- The Honorable Ben Hovland, Commissioner and Chair of the federal Election Assistance Commission ('Federal-State Partnership: Preparing for the 2024 Elections')
- Rene Diresta, Research Manager, Stanford Internet Observatory, Cyber Policy Center. ("Disinformation & Democracy')
- Anne Dames, IBM Distinguished Engineer. ('Quantum Computing: Preparing for the Cybersecurity Threats to Come')
- Jennifer Tang, Tiffany Saade, and Steve Kelley, Institute for Security and Technology. ('Adversarial AI: The Implications of Artificial Intelligence in Cybersecurity')

In addition to the plenary meetings, the Council's six permanent committees met a total of 15 times in public session. The subcommittee members do most of the work in shaping recommendations, providing inputs into cybersecurity bills, participating on working groups, attending stakeholder meetings, and testifying in support of bills during the legislative session. In this work, they benefit from both expert presentations and research conducted by their members and Council staff. During this biennium, for example, various subcommittees received presentations from the Electronic Privacy Information Center (model consumer privacy statute), the California Consumer Privacy Protection Agency (consumer rights enforcement), the New York Department of Health (hospital cybersecurity regulation), the Center for Internet Security (K12 cybersecurity), the National Consortium of Cyber Clinics (clinic models), and the University of Maryland Center for the Governance of Technology and Systems (attack surface of Maryland critical infrastructure).

[17] See Appendix B.

A key resource that the Council was able to 'convene' during the biennium was an NSA employee who was hosted by the Attorney General's Office but worked full-time for the Council for one year. This was at no cost to the State under an external fellowship program that the Agency offers. The Fellow focused on the cybersecurity of the community water service providers serving Maryland and produced a report with more than 50 recommendations.[18] These were endorsed by the Council's Subcommittee on Critical Infrastructure and approved by the Council in plenary session.[19] As discussed in detail below, this report shaped benchmark cybersecurity legislation in the 2025 session.

Finally, during the biennium the Council staffed the Modernize Maryland Oversight Commission (MMOC) and facilitated its work in 2023. The MMOC itself was established by legislation[20] that drew heavily from an earlier Council report on State and local government cybersecurity.[21] By design, MMOC had overlapping membership with the Council (Senator Hester and DoIT Secretary Katie Savage) and the Joint Committee on IT, Cyber, and Biotechnology (Senator Hester and Delegate Kaiser). Ultimately, Council staff organized most of MMOC's 2023 meetings[22] and drafted its initial report. Published in December 2023, the Commission's final report,[23] unanimously approved, drew extensively from the draft and its 20 recommendations. The report impacted two significant State IT bills that were enacted in 2024 and 2025. This is also described more fully below.

Convening to Act: The Council's Supporting Role in State Policymaking & Public Education

As mentioned, the Council focused on five sources of cybersecurity risk to Maryland during this biennium. Its activities in each of these areas mark a continuity of effort with the last biennium. As discussed below, that effort has encompassed the production of reports, help in drafting bills and regulations, participation on working groups, and providing supportive testimony in committee and agency hearings.

[18] Mitroka, Mathew (2025, February 13). Cybersecurity and Maryland's community water and wastewater systems: Analysis and recommendations for the Maryland Cybersecurity Council. https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/04022025-cybersecurity-wastewater-systems-analysis-recommendations.pdf

[19] See the minutes of the February 7, 2025, meeting at https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/03032025-md-cyber-council-feb-7-minutes.pdf

[20] Ch. 243. Acts of 2022 (HB 1205). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB1205/?ys=2022rs The bill was sponsored by Senator Hester and Delegate Patrick Young.

[21] See Yelin, B,. Ames, B. and von Lehmen, G (December 22, 2022). Maryland State and Local Government Cybersecurity – Analysis and Recommendations. SEBC Recommendation 5 (p. 36). https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/maryland-state-and-local-government-cybersecurity-analysis-and-recommendations.pdf

[22] The Commission's meetings can be found at https://doit.maryland.gov/cybersecurity/Pages/immc.aspx. Note that the Commission was renamed and its charger altered in the 2024 legislation.

[23] Modernize Maryland Independent Oversight Commission (2023, December 20). Interim Report. https://doit.maryland.gov/Documents/MMC/MMOC-InitialReport-12202023.pdf

`

Cybersecurity Risk: Utilities and Healthcare

The Council's engagement in these areas included SB 871/HB 1062 (Community Water and Sewerage Systems - Cybersecurity Planning and Assessments [2025]),[24] PSC Rulemaking 76 (RM 76), and SB 691/HB 333 (Healthcare Ecosystem Stakeholder Cybersecurity Workgroup [2025]).[25]

- Senate Bill 871/House Bill 1062 (Community Water and Sewerage Systems - Cybersecurity Planning and Assessments [2025]

  Signed by Governor Moore in May, this bill was sponsored by Senator Katie Fry Hester and Delegate Harrison. The statute fills a gap in federal law that already regulates water service providers but does not specifically address cybersecurity.[26] Maryland is only one of a very few states to date to take this step.[27]

  The sponsors drew heavily from the 2024 report by the NSA Fellow for the Council on the cybersecurity of community water service providers serving Maryland residents.[28] Beyond the report itself, members of the Council, its staff, and the NSA Fellow assisted with the bill drafting and participated in meetings led by the bill sponsors with the Maryland Department of the Environment (MDE),[29] the Department of Information Technology (DoIT), the Maryland Association of Counties, the Maryland Municipal League, and several water districts, among others. They also provided testimony at the sponsors' request in committee hearings.

  The report's recommendations cover five areas. These include governance and policy, foundational cybersecurity, risk management and resilience, resource management, and cybersecurity education and awareness. How the recommendations influenced the Act is highlighted below.

  The Act empowers MDE to promulgate cybersecurity standards for community water service providers (Report Recommendation 3). It requires MDE to include cybersecurity awareness as part of operator and superintendent certification (Recommendation 2) and for DoIT to establish a list of approved cybersecurity training programs from which community water service providers can select (Recommendation 42). MDE must also mandate that community water service

---

[24] Ch. 495. Acts of 2025 (SB 871/HB 1062). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0871
[25] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0691
[26] Jones, D. (2023, October 16). EPA rescinds rule to include cybersecurity in water system audits after legal challenge. Cybersecurity Dive. https://www.cybersecuritydive.com/news/epa-rescinds-cybersecurity-water-system/696744/
[27] As of this writing, the only other state that appears close to enacting a similar statute is Indiana. See Indiana Senate Enrolled Act of 2025 at https://legiscan.com/IN/text/SB0459/2025
[28] See Note 15 supra. The statute incorporates more than half of the 51 recommendations made in the report.
[29] MDE already had a cybersecurity plan that was aligned in many ways with SB 871/HB 1062 and was seeking regulatory authority to implement it. The plan influenced some elements of the final bill, such as self-certification of compliance by community water service providers. See State of Maryland Cybersecurity Action Plan for Water and Wastewater Systems (2024, June). https://mgaleg.maryland.gov/cmte_testimony/2025/eee/1U7OZ41ZDK1sVYLGLeM_NJ5A6T88vgfPp.pdf

providers protect the list of operators on its website (Recommendation 14) and report cybersecurity incidents (Recommendation 7).

The Act provides that community water providers must identify a primary cybersecurity point of contact for MDE (Recommendation 11) and participate in annual cybersecurity training (Recommendation 8). In addition to requiring that they adopt the standards promulgated by MDE, the Act specifies that community water service providers must commit to adopting zero trust network architecture (Recommendation 19). Every two years, community water service providers must conduct a maturity assessment against the cybersecurity standards (Recommendation 4). They must also have contingency plans to manage cyber disruptions (Recommendation 27).

The Act requires DoIT and the Maryland Department of Emergency Management (MDEM) to assist MDE with some of its responsibilities. DoIT must define the minimum cybersecurity standards and the guidelines and procedures for incident reporting and permit these providers to join the State Information Sharing and Analysis Center (Recommendation 47). The Office of Security Management in DoIT must collect the maturity assessments and provide certain reports to the State CISO. In consultation with the State CISO, MDEM's Cyber Preparedness Unit must provide guidance to local emergency management organizations for incidents against community water service providers (Recommendation 31).

Finally, in other language, the Act expresses the intent of the General Assembly that MDE work with DoIT to conduct a general education campaign of the value of security over remediation for leaders within the community water service sector using specified NIST and CISA resources (Recommendations 21, 22, 28). The language also intends that MDEM prioritize tabletop exercises focused on water cybersecurity (Recommendation 29) and that MDE work with departments and agencies at the federal level among other organizations to identify and access resources available for local community water services (Recommendation 36).

- *Public Service Commission Rulemaking 76* (RM 76).

The purpose of this 2024 rulemaking was to implement the Critical Infrastructure Act of 2023[30] sponsored by Senator Hester and Delegate Lily Qi. This statute originated in an earlier Council report on the electric grid serving Maryland[31] and incorporated many of that report's recommendations. The Council continued its involvement with the 2023 legislation by participating in the rulemaking proceeding last year.

Specifically, members of the Council and its staff submitted extensive comments[32] on key questions identified by the Commission's Cybersecurity Rulemaking Working Group (CSRWG).

[30] Ch. 499. Acts of 2023. (HB 969). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0969/?ys=2023rs

[31] This report was the work product of an earlier NSA Fellow attached to the Council. See Corcoran, L (2022, December). Cybersecurity and the Maryland Electric Grid at https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/cybersecurity-and-the-maryland-electric-grid.pdf

[32] Abeles, J., Draffin, C., Hayes, T., von Lehmen, G (2024, March 13). In RE RM 76: Comments by members and

`

They also participated in both onsite and virtual meetings convened by the Commission. This activity was in tandem with a letter from Senator Hester to clarify certain aspects of the statute the Commission was asked to implement.[33] The Council's submission addressed questions raised in the working group meetings about federal preemption of State regulation, cybersecurity incident reporting, and zero trust implementation. The submission by Council members and staff benefitted from information shared by the Federal Electric Reliability Corporation (FERC) and the North American Electric Reliability Corporation (NERC).

The final rules published by the Commission in December 2024 were consistent with the position of Council members and its staff. The Commission's final rules adopted the Council members recommendations for the definitions of "zero trust" and a "cybersecurity incident". They also incorporated their suggested language for evidence of zero trust implementation by the covered entities.[34]

- *Senate Bill 691/House Bill 333 (Healthcare Ecosystem Stakeholder Cybersecurity Workgroup [2025]).*[35]

While this bill did not become law, the Council was involved in the process to shape it. The purpose of the bill was to address the systemic risks exposed by the disruptive Change Healthcare ransomware attack.[36] The event highlighted the fact that the reliability of patient care not only depends on the cybersecurity of individual primary care providers but also on that of the various intermediaries critical to the primary care system. Sponsored by Senator Hester and Delegate Kenneth Kerr, the 2025 bill originally had two broad objectives: a) to convene a workgroup to map the interdependencies within the healthcare ecosystem serving the State and to identify the essential capabilities of entities within the ecosystem that must function to ensure patient care in a cyber attack or other crisis, and b) to enable the Maryland Healthcare Commission (MHCC) and the Maryland Insurance Administration (MIA) to issue regulations to enhance the cybersecurity of those capabilities across the ecosystem. In its final form, the bill was amended to provide for the working group alone.

The original bill was the product of a working group led by Senator Hester which included Council members, a former member, Council staff, and stakeholders whom Senator Hester invited to participate.[37] Council contributions included participation in stakeholder meetings with the Maryland Hospital Association, the Maryland Insurance Agency, and individual hospitals, among others, and providing testimony in the legislative committees. The Center for Health and Homeland Security (CHHS) at the University of Maryland, Baltimore, one of the participating

---

staff of the Maryland Cybersecurity Council at https://webpscxb.psc.state.md.us/DMS/rm/RM76

[33] Office of Senator Katie Fry Hester (2024, March 13). In RE RM 76. https://webpscxb.psc.state.md.us/DMS/rm/RM76

[34] See COMAR 20.06.01.02 and 20.06.01.06 at https://dsd.maryland.gov/regulations/Pages/20.06.01.02.aspx and https://dsd.maryland.gov/regulations/Pages/20.06.01.06.aspx

[35] See https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0691

[36] Whittaker, Zack (2025, January 27). How the ransomware attack at Change Healthcare went down: a timeline. https://techcrunch.com/2025/01/27/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/

[37] See April 3, 2024, letter to the Maryland Hospital Association. https://1drv.ms/f/c/da0790498ca8843a/EnZLjfMrZzFAiVI1-wW7smwBMX9n0WoLStvxAlYfP_sF6g?e=rTeSd6

`

Council members, also produced a background report on healthcare cybersecurity to inform the stakeholder meetings.[38]

Risk and Legacy State IT

Senator Hester and Delegate Kaiser sponsored bills in 2024 and 2025 to address the cybersecurity risks of legacy IT by requiring changes to enable the State Executive Branch to more easily modernize its systems. These bills are SB 982/HB 1188 (Information Technology - Modernization of Information Technology Projects) and SB 705/HB 738 (Department of Information Technology - Major Information Technology Development Projects – Oversight), respectively. Both were enacted.[39]

These bills were informed by the 2023 final report of the MMOC which was drafted by Council staff and answered concerns discussed in an earlier Council report about the cybersecurity risks of State legacy IT systems. Broadly, the MMOC report recommended that the State Executive Branch move closer to an enterprise model for IT investment and management with DoIT at the center to reduce duplication and achieve economies of scale. The report addressed how IT investment decisions should be made, funded, and managed. It also called for an external review of IT procurement processes and for public transparency about the progress of IT modernization. These recommendations were grounded in models and practices at the federal level and in other states.

The impact of the report can be seen in examples from each of the two modernization statutes.

- Senate Bill 982/House Bill 1188 includes provisions that establish a procedure for expedited projects (Report Recommendation 1); require DoIT to accomplish the foundational inventory of legacy IT systems across the Executive Branch (Recommendation 1.2); require DoIT to adopt an IT investment maturity model to guide modernization decisions (Recommendation 2); give the DoIT Secretary more responsibility and authority over agency IT acquisitions (Recommendation 4.3) and mandate an external review of the State's current procurement processes to identify where they could be more nimble (Recommendation 5.2).

- Senate Bill 705/House Bill 738 carries forward a number of recommendations of the 2023 report. Examples include reiterating the Secretary's oversight of the implementation of major IT development projects (MITDPs) across the Executive Branch (Recommendation 4.3); increasing the Secretary's control over agency acquisitions of any IT services or products (Recommendation 4.3); and providing for public transparency about the progress of IT modernization (Recommendation 3.1).

[38] Hart, Chris (2024, July). Review of National and State-Level Data Relating to Cyber Incidents and Cybersecurity at Healthcare Organizations. Center for Health and Homeland Security (CHHS), University of Maryland, Baltimore. https://1drv.ms/b/c/da0790498ca8843a/ETqEqIxJkAcggNq2gwAAAAABkiDzGtFrj5vMefTmvsNX0w?e=b7UdoD

[39] Ch 497. Acts of 2024 (SB 982/HB 1188) at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0982/?ys=2024rs and Ch, 846. Acts of 2025 (SB 705/HB 738). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0705

`

The Talent Gap: Cybersecurity Workforce Development

Enacted in 2025, *SB 867/HB 1468 (Cyber Maryland Program – Revisions),*[40] was sponsored by Senator Hester and Delegate Catherine Forbes. The statute was the second in as many years to amend the law that established the CyberMaryland Program in 2023.[41] The Council has been involved throughout this legislative history, starting with a cyber workforce development recommendation in 2021.[42]

The CyberMaryland Program was established at the Maryland Technology Development Corporation (TEDCO) to be the cybersecurity workforce development hub for the State.[43] Its overarching mission is to pull together all stakeholders within the State—industry groups, the postsecondary sector, State entities, and nonprofits—to work as partners to close the talent gap. This is reflected in its advisory board that includes these stakeholders. To accomplish its mission, the Program's charter requires it to conduct real-time research on workforce needs and to use that research to inform a workforce development strategic plan that will "develop, promote, support, and invest" in talent improvement initiatives, such as those based on the US Chamber of Commerce Talent Pipeline Development Model. To date, the Program has completed its first research report on workforce need and produced a strategic plan jointly with the Governor's Workforce Development Board.[44]

The 2025 bill effected a number of changes. These include moving the Program from TEDCO to the Maryland Department of Labor, providing for competitive grants consistent with the strategic plan, and specifying an expansive list of eligible grant recipients. The legislation also authorized the Governor to request $3.1M Program funding for FY 2026 and provided that $1M of that funding "may" be allocated for cyber clinics, including those focused on operational technology in critical infrastructure. In a related action, the General Assembly approved the $3.1M for the Program.[45]

In a run-up to the 2025 legislative session, the Council organized a series of four meetings at Senator Hester's request to look at the current state of play across the nation relevant to cyber workforce development. These meetings included presentations by CyberFlorida about the outcomes of its $12 million cyber pathways grant program; the Newark, New Jersey, School

---

[40] Ch. 218, Acts of 2025 (SB 867/HB 1188). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0867

[41] The Act establishing the CyberMaryland Program was Ch. 578. Acts of 2023 (SB 801/HB 1188). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0801/?ys=2023rs. This statute was in turn amended by Ch, 509. Acts of 2024 (SB 816/HB 1146). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0816/?ys=2024rs

[42] See Appendix B, 2021 Recommendation 5.

[43] See testimony of Senator Hester at https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0350 https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=fin&ys=2023RS&clip=FIN_3_7_2023_meeting_1&billNumber=sb0801 and Delegate Forbes at https://mgaleg.maryland.gov/cmte_testimony/2023/hgo/14973_03072023_81151-543.pdf

[44] The research report (Cyber Workforce Analysis and Strategy) and the strategic plan (Maryland's Cyber Talent Strategy Plan) can both be found at https://www.tedcomd.com/resources/government-program-development-affairs-policy/cyber-maryland-program

[45] Ch. 602. Acts of 2025 (HB 350). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0350?ys=2025RS

District, about the use of AI tutors in STEM education; and the Consortium of Cyber Clinics about how to establish college or university student clinics to provide hands-on experience through pro bono work for small businesses and local governments. Beyond these meetings, Council members also supported SB 867/HB 1468 through testimony in the committee hearings.

Consumer-related Cybersecurity Risk

Council member organizations sponsored and participated in three webinars directed at the general public on cybersecurity topics.[46] One of these, hosted by the CASH Campaign of Maryland in the fall of 2023, concerned cybersecurity hygiene ('Don't get Tricked by Cyber Criminals'). Two others in 2024—one hosted by the CASH Campaign and the other by the University of Maryland Global Campus—included Senator Sara Love and focused on the consumer rights provided by the Maryland Online Data Privacy Act of 2024 (MODPA).[47] The Council also organized a plenary session discussion at the December 2023 CyberMaryland conference with Senator Hester and Senator Love to talk about the critical infrastructure security and consumer privacy issues of concern to them.

The MODPA realized a long-standing Council recommendation that Maryland provide at least the same consumer rights with respect to sensitive data held by private entities that residents of California—the benchmark in this area—enjoy.[48] The large datasets of personal information held by private entities constitutes a cybersecurity exposure for consumers. By codifying more consumer rights with respect to their data, the MODPA enables them to reduce this exposure. Members of the Council and Council staff supported the legislation in the 2024 committee hearings.

Looking Ahead

As transformative technologies, quantum computing (QC) and artificial intelligence (AI) present new cybersecurity and other closely related risks. The threats from QC are prospective but near term. Estimates are that "Q-Day", when a true quantum machine is built and operating, is expected before 2035.[49] The risks are steep. Current practices for authentication and confidentiality will not withstand quantum machines. Passwords and encryption that classical computers need hundreds of years to break will be breakable by quantum machines in much shorter timeframes, such as minutes or hours. "[E]verything could become vulnerable, for everyone".[50]

[46] The webinar descriptions and participants can be found at https://mdcashacademy.org/event/dont-get-tricked-by-cyber-criminals/; https://mdcashacademy.org/event/marylands-new-online-data-privacy-act-what-you-need-to-know/; and https://www.umgc.edu/cybersecurity/center-for-security-studies/cyber-awareness-month

[47] HB 567/SB 541 (Maryland General Assembly, 2024 Session). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0567/?ys=2024rs

[48] See Appendix B, 2021 Recommendation 2.

[49] Katwala, A. (2025, March 24). The quantum apocalypse is coming: be very afraid. Wired. https://www.wired.com/story/q-day-apocalypse-quantum-computers-encryption/

[50] Ibid.

`

The risks presented by AI are already being felt. Some of these—like the unguarded exposure of sensitive data—can be the result of shortcomings within the AI development lifecycle.[51] Other risks, however, stem from the malicious exploitation or malicious use of AI. AI models are susceptible to manipulation to reveal sensitive information or to cause disruption.[52] Deepfakes created by AI tools can and have been used as a highly sophisticated form of business compromise[53] and to abuse the privacy interests of individuals by being sharing through email or social media.[54] On the horizon are attacks by AI agents or teams of agents that will offer the scale, speed, nimbleness, and effectiveness that bot-driven attacks do not have.[55]

Given the trajectory of these technologies, the General Assembly amended the Council's charter in 2025 to name these risks and to ensure that they would be within the scope of the Council to consider.[56] The amendment mandates that the Council "assess and address" not only cybersecurity threats from artificial intelligence and quantum computing but also the "associated risks" of these technologies. The amendment calls out a number of these risks. It specifies the "cybersecurity and associated risks" to "the sensitive privacy interests of State residents". It lists emerging threats, including AI's use for adversarial AI, deepfakes, and otherwise unethical or fraudulent purposes. To help effect these ends, the amendment provides for the invitation of additional members with relevant expertise. It also allows the Council to elect its chair who may appoint additional members as appropriate.

As highlighted by the General Assembly, and unless pre-empted by federal law,[57] both of these risks will be priorities for the Council in the biennium ahead. In its last session, the General Assembly also established a consumer protection workgroup on AI implementation. To maximize the efforts of both bodies, the statute requires that the two bodies coordinate their work as agreed by the respective chairs.[58]

---

[51] See NIST (2023, January 26). AI risk management framework. AI RMF-1.0. https://www.nist.gov/itl/ai-risk-management-framework

[52] Vassiliev, A., et al. (2024, January). Adversarial machine learning: A taxonomy and terminology of attacks and mitigations. NIST. AI 100-2e2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf

[53] Cox, J (2025, April 28). The age of realtime deepfake is here. 404 Media. https://www.404media.co/the-age-of-realtime-deepfake-fraud-is-here/

[54] Looker, R (2024, April 26). Baltimore high school teacher arrested over deepfake racist audio of principal. BBC. https://www.bbc.com/news/world-us-canada-68907895?ref=404media.co ; Cole, S (2024, September 26). Schools are failing to protect students from nonconsensual deepfakes, report shows. 404 Media. https://www.404media.co/schools-are-failing-to-protect-students-from-non-consensual-deepfakes-report-shows/ The fact that social media platforms can be used in this manner is a vulnerability, "a condition that enables a threat event to occur". See NIST Glossary at https://csrc.nist.gov/glossary/term/vulnerability

[55] Williams, R (2025, April 4). Cyberattacks by AI agents are coming. MIT Technology Review. https://www.technologyreview.com/2025/04/04/1114228/cyberattacks-by-ai-agents-are-coming/ . See also Zu, Y, et al. (2025, April 10). CVE-Bench: A benchmark for AI Agents' ability to exploit real-world web application vulnerabilities. arXiv:2503.17332 [cs.CR]. https://arxiv.org/pdf/2503.17332

[56] Ch. 628. Acts of 2025 (SB 294). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0294

[57] See Lee, A., et al. (2025, May 28). US House of Representatives advance unprecedented 10-Year moratorium on state AI laws. National Law Review. https://natlawreview.com/article/us-house-representatives-advance-unprecedented-10-year-moratorium-state-ai-laws. Among many groups, the National Association of State CIOs (NASCIO) has taken a strong stand against this provision in the House bill. See its May 13, 2025, press release at https://www.nascio.org/press-releases/nascio-statement-on-efforts-to-prevent-state-enforcement-of-ai-laws-for-ten-years/

[58] Ch. 105, Acts of 2025 (HB 956). https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0956

`

Conclusion

As the Presidential Executive Order 14239 indicates, less direct federal support for state and local cybersecurity is to be expected for the foreseeable future.[59] At this writing, the reauthorization of State and Local Cybersecurity Grant Program is very much at risk.[60] The US Department of Homeland Security has discontinued funding for the Election Information and Analysis Center and the Multi-State Information and Analysis Center.[61] The latter program has provided cyber threat intelligence and cyber incident response services to more than 100 public entities in Maryland and more than 15,000 nationwide.[62] Pacing these changes are the planned workforce reductions at CISA, including its regional centers, which have been announced as a refocus on core missions.[63] But the impact of these on the states, if they occur, is unclear.

At the same time, federal regulatory activity in general, including that related to cybersecurity risks to critical infrastructure, individual privacy, and AI, has been paused and is under review. In some cases, regulations have been rescinded.[64] Meanwhile, increased Executive control of independent agencies is a question before the courts and could potentially provide more direct opportunity to reduce regulatory activity over the next several years.[65]

On the other hand, workforce development, a long-standing focus of the Council, is already seeing "a significant shift in how American students will prepare for future technology careers."[66] The announced AI education initiative for K12 schools is characterized as "a comprehensive initiative [that] aims to build essential AI literacy and skills from an early age,

---

[59] See Executive Order 14239 (2025, March 18). Achieving Efficiency Through State and Local Preparedness. Federal Register 2025-04973 (90 FR 13267). https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness

[60] June 3, 2025, email communication with staff at the National Association of State CIOs.

[61] Wood, C. (2025, March 11). MS-ISAC loses federal support for threat intelligence, incident response. Statescoop. https://statescoop.com/ms-isac-loses-federal-support/

[62] See Note 20, supra, page 20.

[63] Riotta, C. (2025, June 6). 'There will be pain': CISA cuts spark bipartisan concerns. Data Breach Today. https://www.databreachtoday.com/cisa-braces-for-major-workforce-cuts-amid-security-fears-a-27996?highlight=true

[64] See for example, Executive Order 14192 (2025, January 31). Unleashing Prosperity through Deregulation. 2025-02345 (90 FR 9065). https://www.federalregister.gov/documents/2025/02/06/2025-02345/unleashing-prosperity-through-deregulation; Executive Order 141179 (2025, January 23). Removing Barriers to American Leadership in Artificial Intelligence. 2025-02172 (90 FR 8741). https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence; and Jacobson, J., et al. (2025, February 11). A new era: Trump 2.0 highlights for privacy and AI. National Law Review. https://natlawreview.com/article/new-era-trump-20-highlights-privacy-and-ai

[65] Howe, A. (2025, May 22). Supreme Court allows Trump to remove agency heads without cause for now. SCOTUSblog. https://www.scotusblog.com/2025/05/supreme-court-allows-trump-to-remove-agency-heads-without-cause-for-now/

[66] Hernholm, S. (2025, April 22). Trump Signs Executive Order For AI Education For K-12 Schools. Forbes. https://www.forbes.com/sites/sarahhernholm/2025/04/24/trump-signs-executive-order-for-ai-education-for-k-12-schools/. See Executive Order 14277 (2025, April 23). Advancing Artificial Intelligence Education for American Youth. 2025-07368 (90 FR 17519). https://www.federalregister.gov/documents/2025/04/28/2025-07368/advancing-artificial-intelligence-education-for-american-youth

`

positioning the United States to maintain its competitive edge in global technology development and prepare students for an AI-driven economy."[67]

The impact of some of the foregoing changes will be quickly felt. In other cases, the impacts are uncertain and will take time to unfold. As always, the activity of the Maryland Cybersecurity Council will be responsive to its charter, the risks, and the gaps in federal policy.

More Information

Questions about the report may be addressed to:

University of Maryland Global Campus
ATTN Maryland Cybersecurity Council Staff
3501 University Boulevard East
Adelphi, Maryland 20783
Marylandcybersecuritycouncil@umgc.edu

[67] Ibid, Hernholm.

Appendix A

Council Subcommittees and Appointed Members

Fiscal Years 2024 – 2025

Council Subcommittees and Appointed Members

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

- Chair: Blair Levin, Nonresident Senior Fellow, Metropolitan Policy Program, Brookings Institution
- Michael Greenberger, Professor, Francis Carey School of Law, University of Maryland, Baltimore
- Joseph Morales, Esq., The Morales Law Firm
- Keith Moulsdale, Esq., Attorney, Whiteford, Taylor & Preston
- Vanessa Purnell, Associate Vice President, Government Affairs, Medstar Health
- Markus Rauschecker, Director, Center for Health and Homeland Security, University of Maryland, Baltimore.

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: Katie Savage, Secretary of the Department of Information Technology
- Robin Morse, National Security Agency, Liaison to the Council
- Kristin Jones Bryce, Vice President of External Affairs, University of Maryland Medical System
- Russell Strickland, Secretary, Maryland Department of Emergency Management
- Robert W. Day Sr., Senior Project Manager, Howard University
- Jared DiMarinis, State Administrator, State Board of Elections
- Travis Nelson, Director, Governor's Office of Homeland Security
- Anthony Lisuzzo, President Emeritus, Army Alliance
- Major General Janeen Birckhead, Adjutant General, Maryland Military Department

- Major Tawn Gregory, CIO, Maryland Secretary of State Police
- Russell Strickland, Secretary, Maryland Department of Emergency Management

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: John Abeles, President and CEO, System 1, Inc.
- Vice Chair: Cyril Draffin, Project Advisor to the Massachusetts Institute of Technology (MIT) Energy Initiative
- Dr. David Anyiwo, Chair, Department of Management Information Systems, Bowie State University
- Terri Jo Hayes, Executive Consultant, Mfusion, Inc.
- Ryan Hsu, Esq., Counsel, Maryland People's Counsel
- Markus Rauschecker, Director, Center for Health and Homeland Security, University of Maryland, Baltimore
- Roberto Suarez, Vice President, Architecture, Planning, and Security, CareFirst
- Rhyner Washburn, Threat Intelligence Analyst, Maryland Coordination and Analysis Center

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
- Tasha Cornish, Executive Director, Cybersecurity Association of Maryland (CAMI)
- Dr. Michel Cukier, Associate Professor and Director, ACES, University 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
- Kimberly Mentzel, Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- 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, U.S. 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 tax incentives

Subcommittee Members
- Chair: Belkis Leong-Hong, Founder, President, and CEO, Knowledge Advantage, Inc.
- Tasha Cornish, Executive Director, Cybersecurity Association
- Mary Kane, CEO, Maryland Chamber of Commerce
- Brian Israel, Business Development, Strategy, Corporate Finance, Forvis
- Mathew Lee, CEO, Fastech
- Larry Letow, President, US Region, CyberCX
- Kimberly Mentzel, Director, Office of Cybersecurity and Aerospace, Maryland Department of Commerce
- Jill Porter, Director, AADC, for the Maryland Tech Council
- Troy Stoval, CEO/Executive Director, Maryland Technology Development Corporation (TEDCO)
- Steven Tiller, President, Fort Meade Alliance Foundation

Subcommittee on Public Awareness and Community
Subcommittee Objectives

- Promote the Council's objectives and spread awareness of the 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, CASH Campaign of Maryland
- Anton Dahbura, PhD, Executive Director, Information Security Institute, Johns Hopkins University
- Jayfus Doswell, PhD, Founder, President, and CEO, The Juxtopia Group, Inc.

APPENDIX B

Recommendations of the

Maryland Cybersecurity Council

Fiscal Years 2016 – 2025

`

Recommendations of the Maryland Cybersecurity Council

Fiscal Years 2016 – 2025

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 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.	

	Recommendations in the 2017 Biennial Report (Continued)	Originating Subcommittee
3.	Legislation requiring express consumer consent for internet service providers (ISPs) to sell or transfer consumer internet browser history. (Replaced 2021 Recommendation 2).	
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 the 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.	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 businesses 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.	

	Recommendations of the 2021 Report Continued	
7.	Implementing a tax credit analysis in coordination with the Maryland Department of Commerce to review 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 receiving available tax credits. Mindful of the competing demands on the state, but with an eye to supporting growth in the state's business base, the Council further recommends that so much as possible relevant existing tax credits be extended to provide longer availability and available funds for existing tax credits be increased.	

	Recommendations of the 2023 Report	
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

`

2023 Biennial Report Recommendations from Sponsored Research
See Appendix B in Cybersecurity and the Maryland Electric Grid – Findings and Recommendations. https://www.umgc.edu/content/dam/umgc/documents/upload/cybersecurity-and- the-maryland-electric-grid.pdf
See Appendix B in State and Local Government Cybersecurity – Analysis and Recommendations. https://www.umgc.edu/content/dam/umgc/documents/upload/maryland-state-and- local-government-cybersecurity-analysis-and-recommendations.pdf
See Executive Summary in Report of the Ad Hoc Subcommittee on Consumer and Child Privacy. https://www.umgc.edu/content/dam/umgc/documents/upload/12192022consumer- digital-privacy-recommendations.pdf

2025 Biennial Report Recommendations from Sponsored Research
See Appendix A in Cybersecurity and Maryland's Community Water and Wastewater Systems: Analysis and Recommendations for the Maryland Cybersecurity Council https://www.umgc.edu/content/dam/umgc/documents/md-cybersecurity-council/04022025-cybersecurity-wastewater-systems-analysis-recommendations.pdf