Testimony for SB 780__von Lehmen__Ad Hoc Committee
Uploaded by: Greg Lehmen
Position: FAV

FAVORABLE

TESTIMONY PRESENTED TO THE
SENATE EDUCATION, HEALTH AND ENVIRONMENTAL AFFAIRS COMMITTEE

SENATE BILLS 780 (CYBERSECURITY GOVERNANCE ACT OF 2022) AND SB 812
(CYBERSECURITY – COORDINATION AND GOVERNANCE)

DR. GREG VON LEHMEN
UNIVERSITY OF MARYLAND GLOBAL CAMPUS
MEMBER AD HOC COMMITTEE ON STATE AND LOCAL CYBERSECURITY
POSITION: SUPPORT

MARCH 3, 2022

Chairman Pinsky, Vice Chairwoman Kagan, and Members of this Committee, thank you for the opportunity to submit testimony in support of SB 780 and SB 812.

I am Dr. Greg von Lehmen, University of Maryland Global Campus and staff to the Maryland Cybersecurity Council. I am providing testimony as a member of the Council's Ad Hoc Committee on State and Local Cybersecurity whose report was published in January.

I urge the Committee to support both SB 780 and SB 812 in a unified version for the following reasons.

First, the consolidation of responsibility for cybersecurity and IT that these bills propose would address challenges that DoIT faces in providing cybersecurity for the State Executive Branch. These challenges include a lack of visibility into systems and applications used by departments, compliance with the State Security Manual, their cybersecurity budgets, staffing, and security priorities, among other things. What cannot be seen cannot be secured. Unifying responsibility for cybersecurity in DoIT would reduce these challenges.

Second, the consolidation of cybersecurity and IT responsibilities in DoIT would enable the State to reap not only greater security but to see more clearly where economies of scale and lower costs for IT and security applications, systems, and services can be attained by implementing common systems across Executive Branch departments.

Third, this consolidation would allow departments and agencies to focus on why they were created—their business or service mission—rather than requiring them to split management and staff time and attention on maintaining and securing their IT infrastructure.

Finally, in implementing a consolidated model, DoIT would have several advantages. It has an extensive amount of survey data that was collected from the departments as part of the ad hoc study to help it establish priorities. It will have an enhanced governance group, the Maryland Cyber Coordinating Council, a representative body of Executive Branch department heads, to provide advice and counsel. Importantly, it has the experience of other states to learn from. As examples, both Vermont and North Dakota have centralized the provision of their IT and

cybersecurity and provided testimony last year to the Joint Committee on IT, Cybersecurity and Biotechnology regarding the benefits that they have experienced.[1]

The purpose of the Ad Hoc Committee study was to take an objective look at the challenges faced by DoIT in serving the Executive Branch. The committee included CHHS, MDEM, DoIT, and MACo. Its work was supported by testimony from many other groups last year before the Joint Committee on IT, Cybersecurity, and Biotechnology. An effort was made to learn as much as possible from states, with interviews conducted outside of the hearings with CISOs and CIOs in New Hampshire, New Jersey, and North Dakota. The National Governor's Association, the National Association of State CIOs, and the nonprofit Center for Internet Security, among others, were all consulted. Such a study presents the State with a unique opportunity to move forward in an informed way.

For the good of Maryland, I urge the committee to support a consolidated version of SB 780 and SB 812.

Thank you.

[1]See testimony provided to the Joint Committee by Mr. John Quinn (State of Vermont CIO) on June 23, 2021 and by Mr. Shawn Riley (State of North Dakota CIO) on September 29, 2021, at https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_6_23_2021_meeting_1&ys=2021rs, https://mgaleg.maryland.gov/mgawebsite/Committees/Media/false?cmte=mjm&clip=MJM_9_29_2021_meeting_1&ys=2021rs

SB 780_FAV_MML.pdf
Uploaded by: Justin Fiore
Position: FAV

Maryland Municipal League

The Association of Maryland's Cities and Towns

TESTIMONY

March 3, 2022

Committee: Senate Education, Health and Environmental Affairs Committee

Bill: SB 780 – Cybersecurity Governance Act of 2022

Position: Support

Reason for Position:

The Maryland Municipal League supports SB 780, which would establish a new cybersecurity framework in the State that includes local coordination, technical support, and financial assistance to local governments rising to meet modern threats.

Cities and towns are grateful to the sponsors for their leadership and nuanced approach to establish the tools and resources necessary to assist the State and local governments in a comprehensive manner. We believe this is a great example of a State and local partnership to protect our shared constituencies.

The Maryland Municipal League therefore respectfully requests the Committee provide SB 780 with a favorable report.

FOR MORE INFORMATION CONTACT:

Scott A. Hancock	Executive Director
Angelica Bailey	Director, Government Relations
Bill Jorch	Director, Research & Policy Analysis
Justin Fiore	Manager, Government Relations

SB780_812 - Cybersecurity Governance Act of 2022.p
Uploaded by: Katie Fry Hester
Position: FAV

KATIE FRY HESTER
Legislative District 9
Carroll and Howard Counties

Education, Health, and
Environmental Affairs Committee

Chair, Joint Committee on
Cybersecurity, Information Technology
and Biotechnology

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
James Senate Office Building
11 Bladen Street, Room 304
Annapolis, Maryland 21401
410-841-3671 · 301-858-3671
800-492-7122 *Ext.* 3671
KatieFry.Hester@senate.state.md.us

Sponsor Testimony - SB780/812 - The Cybersecurity Governance Act of 2022

March 3, 2022

Thank you Chair, Vice Chair, and members of the committee for your consideration of SB780/812 - The Cybersecurity Governance Act of 2022 - which codifies roughly 20 recommendations from the Maryland Cybersecurity Council's (MCC) Report on State and Local Government Cybersecurity Capacity.

As you heard during our January 27th briefing, During the 2021 interim, the Maryland Cybersecurity Council subcommittee studied the threat posed by cybercrime to state & local governments. The subcommittee included the Maryland Department of Information Technology, The Maryland Department of Emergency Management, the University of Maryland Center for Health & Homeland Security, the Maryland Association of Counties (MACo), and the Maryland Municipal League (MML). I have uploaded a copy of this report with my testimony today.

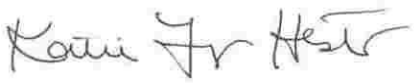
Over the past several years, Maryland has faced significant challenges as a result of cyberattacks at the state and local level. From our state agencies, to school systems, and municipal agencies, the need has never been greater to improve our state's capacity to implement and enforce IT and cybersecurity policy. This legislation addresses the decisions that must be made about threats, including who should be responsible for making them, how those decisions should be informed, and most importantly, and how they should be implemented and evaluated. It achieves these goals by:

1.) Codifying the roles of the State Chief Information Security Officer (SCISO) and the Maryland Cybersecurity Coordinating Council (MCCC),
2.) Centralizing IT and cybersecurity functions and funding under the Department of Information Technology (DoIT), which may take six months to develop and two years or so to implement,
3.) Establishing an advisory group to develop and oversee the implementation of a cybersecurity strategic plan,
4.) Requiring each agency to complete annual risk assessments and certify compliance with DoIT,

5.) Appropriating a consistent budget for DoIT (as opposed to the current charge-back model), and
6.) Streamlining the procurement process for cybersecurity and IT contracts, with increased security requirements for contractors who will have access to state databases.

Most importantly, I want to clarify that this centralization and consolidation of IT and cybersecurity systems does not mean that we're going to steal computers out of office buildings and kidnap staff: the day-to-day operations of our state agencies will still carry on as they have been. Ultimately, we envision this as a collaborative and smooth transition process. This bill is complicated, and requires additional refining to clarify drafting errors and to align it with the findings of the MCC Report, so please consider the sponsor amendments that have been offered; however, these recommendations are in line with national trends and cybersecurity best practices. Maryland's cyber governance needs to modernize and evolve as threats to our safety and information evolve. Without this legislation, we will only see the costs of inaction continue to grow. **For these reasons, I respectfully request a favorable committee report .**

Sincerely,



Senator Katie Fry Hester
Howard and Carroll Counties

SB780 - SWA - Cybersecurity Governance Act of 2022

Uploaded by: Ary Amerikaner

Position: FWA

MARYLAND STATE DEPARTMENT OF EDUCATION
EQUITY AND EXCELLENCE

Mohammed Choudhury
State Superintendent of Schools

BILL:	SB780	**DATE:**	March 3, 2022
SUBJECT:	Cybersecurity Governance Act of 2022	**COMMITTEE:**	Education, Health, and Environmental Affairs
POSITION:	Support with Amendments		
CONTACT:	Ary Amerikaner 410-767-0090 ary.amerikaner@maryland.gov		

The Maryland State Department of Education (MSDE) supports with amendments **Senate Bill 780 – Cybersecurity Governance Act of 2022**, which would establish the Office of Security Management within the Department of Information Technology (DoIT), names the head of the new office as the State Chief Information Security Officer (SCISO), creates Directors of Local and State Cybersecurity, establishes the Maryland Cybersecurity Coordinating Council, and amends the definitions of cybersecurity and information technology.

As a custodian of sensitive data for over 900,000 Maryland public school students and thousands of public-school staff, protecting this information is a top priority. MSDE supports strong security protocols. We are fully committed to the cybersecurity goals of the state and support the relevant measures proposed in the legislation. As a DoIT enterprise agency, MSDE staff works with the State Chief Information Security Officers' team regularly. MSDE receives monthly reports from DoIT identifying any vulnerabilities to applications on MSDE's network. MSDE's Information System Security Officer works with stakeholders to mitigate the identified vulnerabilities. MSDE has also worked with DoIT in transitioning identified obsolete IT infrastructure (servers, systems etc.) to a supported platform. At present, MSDE and DoIT are jointly working on a series of cybersecurity assessments to understand the maturity of our data management programs, our security posture, data governance, and security configurations. In addition, MSDE IT leadership has been directed to ensure that security trainings released by DoIT are completed by all staff as they are released. MSDE currently has a contractual security professional from an approved DoIT vendor assigned as Information System Security Officer (ISSO). MSDE is working on establishing a fulltime position, Chief Information Security Officer (CISO), to oversee this work and increase collaboration and coordination with the current and new security processes, protocols and personnel established by DoIT.

However, MSDE has serious concerns that the part of the bill that shifts control of all IT functions to another agency will have an adverse impact on the operations of the Department, undermining our ability to ensure high quality IT support for our employees and constituents. This can be loosely grouped into three related concerns:

1. **Mission aligned support that meets agency timelines and quality standards.** An organization's technology operations go beyond the secure networks and standardized software systems that support operations. It requires IT staff that understands the priorities of the agency

and works to put them in the forefront. The IT staff needs to be keenly aware of the program priorities, laws, regulations and deadlines that drive the work. It is important that they report to the head of the agency who can ultimately ensure that program priorities and customer service expectations are reflected in the IT team's work product.

As part of the new administration's first phase of reorganization, we have utilized existing vacancies in the department to create IT partner positions and structured them to work with their counterparts in other parts of the agency to provide a high quality and continuous customer service to the divisions. Absorbing these newly created positions into DoIT and associated transition will cause disruption and will have negative impact on MSDE's ability to create a high functioning department as we implement the Blueprint for Maryland's Future. Therefore, the language in the bill that broadly defines anyone working more than 50% of their time on IT operations as becoming DoIT employees is concerning.

2. **Specialized knowledge of the field.** The information technology service needs of MSDE range from supporting technology needs of the regional offices in the Division of Early Childhood to supporting high quality data analysis and reporting in research and assessment offices. These needs cannot be effectively met by a centralized operation that is designed to meet the overall needs of many agencies. In one recent example, MSDE submitted an RFP to start a College and Career Ready study. This subject matter is entirely outside of DoIT's core area of work, and yet they must review it, which results in significant involvement from MSDE staff to provide subject matter guidance.

3. **Procedural bottlenecks and timeline delays.** Too often, the structure of a centralized IT support program leads to consistent delays and bottlenecks for agencies. For example, MSDE currently submits all technology procurement requests to the DoIT intake committee for review and approval prior to purchase. When software as a service (SaaS) products are procured, MSDE must submit system control documentation and system security plans prior to receiving an authority to operate from DoIT. As MSDE is one of many customers serviced by DoIT, we have experienced delays in getting the reviews expeditiously. We recently have experienced several week delays in, for example, (a) obtaining a resource for urgently needed website updates and (b) reviewing a high priority Blueprint for Maryland's Future Request for Proposals (RFP).

   While IT staff employed by our department have worked through these limitations to ensure the needs of the department are met, this experience reinforces the MSDE belief that IT staff employed by the agency are critical to our success.

MSDE's experiences and concerns above are not a reflection on the commitment and skills of the DoIT leadership or staff. Instead, they reflect (1) a lack of standardized collaboration norms and service expectations across multiple agencies; (2) an inadequate level of staffing at DoIT to fulfill obligations to their customers; and (3) the impossible task of knowing enough about multiple state agencies' complicated work to meaningfully support their IT needs.

Absorbing the IT operations of the department into DoIT will only exacerbate the challenges outlined above and cause unaccounted disruptions due to transition. This is especially concerning to MSDE as we accelerate into the first few years of meaningful implementation of the Blueprint for Maryland's Future.

MSDE proposes a collaborative approach to mitigate these concerns. This would include amendments that:

- Allow MSDE to retain ownership of existing IT resources;
- Establish regular communication channels between DoIT and the department stakeholders;
- Establish IT hiring standards across all agencies that align with the overall cybersecurity objectives of the state;
- Establish standard evaluation protocols that ensure effective evaluation of the IT resources that align with the security regulations;
- Require IT staff at the agencies complete mandatory minimum trainings each year to stay updated on the latest skill levels required to operate and support mission critical enterprise systems;
- Increase internal and external penetration testing and security analysis;
- Include MSDE personnel as part of the DoIT procurement intake processes related to MSDE IT needs to establish joint ownership of the processes and planning; and
- Explore procurement process efficiencies to reduce the time taken to complete the procurement process

We respectfully request that you consider this information as you deliberate Senate bill 780. Please contact Ary Amerikaner, at 410-767-0090, or ary.amerikaner@maryland.gov, for any additional information.

SB780 - MoserIT - Testimony in Support w Amendment
Uploaded by: Caitlin McDonough
Position: FWA

The Honorable Paul Pinsky
Chair, Senate Education, Health and Environmental Affairs Committee
Miller Senate Office Building, 2 West
11 Bladen Street
Annapolis, MD 21401

TESTIMONY IN SUPPORT WITH AMENDMENT
SENATE BILL 780 – CYBERSECURITY GOVERNANCE ACT OF 2022

Dear Chairman Pinsky and Members of the Committee:

Moser strongly supports the goals of Senate Bill 780. At Moser, our information technology (IT) professionals help agencies transition from aging systems to newer, more efficient technologies and stay on the cutting-edge to provide consulting that keeps up with widely varying and ever-changing regulatory environments. With experts in more than 16 areas of technology, Moser offers a depth of knowledge and expertise unparalleled in the IT industry. Our professionals perform security assessments, system reviews, updates, and maintenance for government systems and design custom solutions to meet the IT challenges unique to government entities.

Government agencies often deal with highly sensitive information, and the public demands their data be protected. Moser's experts can perform security assessments to identify risks and design solutions to eliminate them, making sure that your systems, processes, and data are always secure. The public also expects their government to provide services without fail, and when things go wrong, the problems are often highly visible. Procuring IT experts can help state agenices avoid the negative spotlight with system reviews, updates, maintenance, and design expert solutions to address all process or performance issues.

Moser strongly supports Senator Hester and the Joint Committee on Cybersecurity, Information Technology and Biotechnology's efforts to standardize and strengthen Maryland's cybersecurity efforts in both the public and private sector. Moser particularly supports the provisions of SB780 which centralize the State's governance of ITand cybersecurity for all executive agencies under the Department of Information Technology, including the coordination and procurement of managed cybersecurity services.

In addition to the essential steps toward standardization in cybersecurity and IT efforts included in the bill as introduced, Moser respectfully urges the sponsor and the Committee to consider adding the following language as a standard requirement for IT procurements conducted by all covered state agencies, as part of its overall cybersecurity plan:

REQUIRING THE DISCLOSURE OF ANY NON-PUBLICLY REPORTED FORMAL CORRECTIVE ACTIONS, SECURITY BREACHES, AND LAWSUITS THAT YOUR COMPANY HAS EXPEREINCED UNDER PREVIOUS CONTRACTS IN THE LAST 10 YEARS.

This is a cybersecurity standard that is increasingly incorporated by other states and we urge Maryland to consider the disclosure of this essential information as an element of its cybersecurity efforts, either directly in statute or in procurement regulations promulgated subsequent to the passage of SB780.

Moser thanks the Committee for its consideration of SB780 and the proposed amendment and urges a favorable report on this essential legislation for ensuring the safe and efficient operation of Maryland.

SB0780-EHE_MACo_SWA.pdf
Uploaded by: Dominic Butchko
Position: FWA

MARYLAND Association of COUNTIES

Senate Bill 754 - *Local Government Cybersecurity - Coordination and Operations (Local Cybersecurity Support Act of 2022)*

Senate Bill 780 - *Cybersecurity Governance Act of 2022*

Senate Bill 812 - *State Government - Cybersecurity - Coordination and Governance*

MACo Position: **SUPPORT WITH AMENDMENTS**

To: Education, Health and Environmental Affairs and Budget and Taxation Committees

Date: March 3, 2022

From: Dominic J. Butchko

A strong partnership between the State and local governments is essential for safeguarding critical infrastructure and defending against increasingly complex cyber risks. MACo urges the General Assembly to provide a meaningful and lasting State commitment to bolster cybersecurity and prioritize cyber resilience through collaborative efforts to identify, protect against, detect, and respond to malicious cyber threats.

Hackers are increasingly targeting states and local governments with sophisticated cyberattacks. Securing government information systems is critical, as a cyber intrusion can be very disruptive, jeopardizing sensitive information, public safety, and the delivery of essential services.

MACo advocates for the State to offer additional cyber grant programs, shared service agreements, 24/7 network monitoring, real-time incident response, statewide risk assessments, and a dedicated cybersecurity support fund to help local governments upgrade IT infrastructure. This will ensure an equitable approach to cyber preparedness and resilience across the state.

Legacy systems — outdated digital software or hardware — are generally unable to interact with any newer systems or implement necessary cybersecurity measures to safeguard critical data and sensitive information. As such, MACo urges the State to prioritize updating outdated technology platforms, which is vital for reducing cybersecurity risks, enhancing service delivery, and boosting government transparency and accountability.

Rising cyber liability insurance premiums and fewer insurance carriers have left counties facing difficulty acquiring and renewing coverage by leveraging its purchasing power. MACo believes the State can provide an affordable solution to ensure local governments remain cyber resilient in times of crisis.

By dedicating needed resources and streamlining collaboration, communication, and coordination, the State can help lead local governments, school systems, and critical infrastructure toward a more cyber-secure future.

The work of the Ad Hoc Committee on State and Local Cybersecurity of the Maryland Cybersecurity Council embodied this spirit in its report. The referenced bills deserve continued stakeholder attention to coalesce behind similar principles. MACo and its member counties stand ready to collaborate to develop a cohesive statutory framework to advance these mutual state/local goals, and request a report of **FAVORABLE WITH AMENDMENTS** on SB 754, SB 780, and SB 812.

SB 754, SB 780 & SB 812 - MoCo_Elrich_SWA (GA 22).
Uploaded by: Marc Elrich
Position: FWA

OFFICE OF THE COUNTY EXECUTIVE

Marc Elrich
County Executive

March 3, 2022

TO: The Honorable Paul G. Pinsky
Chair, Education, Health, and Environmental Affairs Committee

FROM: Marc Elrich
County Executive

RE: Support with Amendments:

Senate Bill 754 – *Local Government Cybersecurity – Coordination and Operations (Local Cybersecurity Support Act of 2022)*

Senate Bill 780 – *Cybersecurity Governance Act of 2022*

Senate Bill 812 – *State Government - Cybersecurity - Coordination and Governance*

I am writing to support the enactment of legislation that increases State funding for cybersecurity programs that enhance the ability of local governments to address cybersecurity threats, facilitates constructive coordination between the State and local governments, and strikes a reasonable balance regarding administrative requirements imposed on local cybersecurity officials (e.g., assessments and reporting). The package of bills referenced above contain many provisions that are consistent with these goals and some that are inconsistent.

The County will be working closely with the Maryland Association of Counties as these bills move forward and stands ready to assist the Education, Health, and Environmental Affairs Committee in any way that would be helpful. We have an excellent cybersecurity team that would welcome the opportunity to participate in discussions or provide information as needed.

I respectfully request that the Committee carefully evaluate the differences between the bills so that the Committee can develop a final product that provides meaningful enhancements to State and local cybersecurity efforts without imposing unnecessary, duplicative, or overly burdensome mandates on local governments that divert resources away from critically important cybersecurity efforts.

cc: Members of the Education, Health, and Environmental Affairs Committee

20 - SB 780 - EHEA - BOP - LOSWA.docx.pdf
Uploaded by: State of Maryland (MD)
Position: FWA

Maryland
DEPARTMENT OF HEALTH

Board of Physicians

Larry Hogan, Governor · Boyd K. Rutherford, Lt. Governor · Damean W.E. Freas, D.O., Chair

2022 SESSION
POSITION PAPER

BILL NO.: **SB 780 – Cybersecurity Governance Act of 2022**
COMMITTEE: **Education, Health and Environmental Affairs // Budget and Taxation**
POSITION: **Support with Amendments**

TITLE: **Cybersecurity Governance Act of 2022**

POSITION & RATIONALE:

The Maryland Board of Physicians; the State Acupuncture Board; the State Board of Examiners for Audiologists, Hearing Aid Dispensers, Speech-Language Pathologists and Music Therapists; the State Board for Certification of Residential Child Care Program Professionals; the State Board of Chiropractic Examiners; the State Board of Dental Examiners; the State Board of Massage Therapy Examiners; the State Board of Nursing; the State Board of Examiners in Optometry; the State Board of Pharmacy; the State Board of Physical Therapy Examiners; the State Board of Podiatric Medical Examiners; the State Board of Professional Counselors and Therapists; the State Board of Psychologists; and the State Board of Social Work Examiners
(the Boards) are submitting this letter of support with amendments for Senate Bill (SB) 780 – Cybersecurity Governance Act of 2022.

Cybersecurity is an essential part of state government. Attacks on the Boards' network infrastructure have the potential to seriously hamper Maryland's health care workforce due to delays in licensure, and in extreme cases, can even expose protected data and put Maryland residents directly at risk.

The Boards support the development of policies and best practices to help ensure that the Boards are properly protected from cybersecurity attacks, and to minimize the harm and impact of such attacks when they do occur. The Boards also support creating processes to oversee these policies and ensure they are being properly followed. These steps will help ensure that the Boards can continue protecting the health and safety of Maryland patients through proper licensure and regulation of health care professionals.

However, the Boards are concerned that sections 5 and 6 of SB 780 would divert board resources and personnel away from the boards at a crucial time. The majority of health occupations boards are specially funded and purchase equipment and other information technology resources through funds that are generated by licensure fees. Language found on page 35, lines 17 through 20 would transfer these assets to the Department of Information Technology (DoIT). Not only would this

potentially deprive the boards of vital resources, it would also mean that individual health care practitioners were directly funding DoIT via their licensure fees.

Also concerning is the language found on page 35, lines 26 through 31, which would transfer all employees who are assigned more than 50% of the time to functions related to information technology operations or cybersecurity to DoIT. While the Boards appreciate that some oversight must exist to ensure that IT staff comply with the policies and procedures developed by DOIT, transferring information technology (IT) staff to DoIT would represent a significant loss for the Boards. The Boards rely on full-time IT staff to quickly resolve issues and maintain essential operations. Under SB 780, these vital employees would be required to report to the Secretary of Information Technology and could be reassigned without input from the Boards.

Therefore, the Boards recommend that the Committee adopt the following amendments:

Amendment 1
The Boards recommend inserting the following language on page 35, line 15 after the word "government:" **OTHER THAN A HEALTH OCCUPATIONS BOARD ESTABLISHED UNDER THE HEALTH OCCUPATIONS ARTICLE**

Amendment 2
The Boards recommend inserting the following language on page 35, line 19 after the word "government:" **OTHER THAN A HEALTH OCCUPATIONS BOARD ESTABLISHED UNDER THE HEALTH OCCUPATIONS ARTICLE**

Amendment 3
The Boards recommend inserting the following language on page 35, line 22 after the word "government:" **OTHER THAN A HEALTH OCCUPATIONS BOARD ESTABLISHED UNDER THE HEALTH OCCUPATIONS ARTICLE**

Thank you for your consideration. For more information, please contact Matthew Dudzic, Manager of Policy and Legislation, Maryland Board of Physicians, 410-764-5042, or Lillian Reese, legislative liaison for the Boards, at 443-794-4757 or lillian.reese@maryland.gov.

The opinion of the Boards expressed in this document does not necessarily reflect that of the Maryland Department of Health or the Administration.

Cybersecurity Letter.pdf
Uploaded by: Sara Elalamy
Position: UNF

Court of Appeals of Maryland
Robert C. Murphy Courts of Appeal Building
361 Rowe Boulevard
Annapolis, Maryland 21401-1699

Joseph M. Getty
Chief Judge

March 2, 2022

The Honorable Paul G. Pinsky
Maryland Senate
Miller Senate Office Building, 2 West Wing
11 Bladen St.
Annapolis, MD 21401

The Honorable Shane E. Pendergrass
Maryland General Assembly
Taylor House Office Building, Room 241
6 Bladen St.
Annapolis, MD 21401

Dear Senator Pinsky and Delegate Pendergrass:

I write to you concerning several bills that seek to impose cybersecurity requirements on the Judicial Branch. These bills include:

- **HB0005/SB0107** – This bill would modify Title 10, Subtitle 13 of the State Government Article to apply to the Legislative and Judicial branches, in addition to the Executive Branch, and would require each employee of each unit of State government to complete a cybersecurity training program certified by the Maryland Department of Information Technology ("DOIT").

- **HB0419/SB0390**, **HB1202/SB0754**, and **HB1346/SB0812**, and **SB 0780** – These bills would renumber Title 3A of the State Finance and Procurement Article as Title 3.5, and would add a requirement in it that, if it uses the DOIT telecommunication and computer network, the Judicial Branch must certify annually to DOIT that it is in compliance with DOIT's minimum security standards.

Article 8 of the Maryland Constitution's Declaration of Rights states: "That the Legislative, Executive and Judicial powers of Government ought to be forever separate and distinct from each other; and no person exercising the functions of one of said Departments shall assume or discharge the duties of any other."

In addition, Article IV, § 18 of the Maryland Constitution grants to the Chief Judge of the Court of Appeals administrative authority over Judicial Branch: "The Chief Judge of the Court of Appeals shall be the administrative head of the Judicial system of the State." Information technology practices, including cybersecurity measures, used by Maryland courts to carry out core judicial functions are administrative matters that fall squarely within the Chief Judge's constitutional duties.

The proposed legislation would infringe on the Judiciary's day-to-day functioning and therefore run afoul of the separation of powers requirement. The Court of Appeals has acquiesced to legislative efforts "augment[ing] the ability of the courts to carry out their constitutional responsibilities" in very narrow circumstances—when "at the most, there was but a minimal intrusion" on inherent powers of the Judicial Branch. *Attorney Gen. of Maryland v. Waldron*, 289 Md. 683, 698 (1981). Though the separation of powers requirement is not absolute, legislative action should support courts rather than impose on their ability to function. *Id.* at 699. ("[T]he flexibility that inheres in the separation of powers doctrine allows for some limited exertion of legislative authority. As a consequence of this elasticity, [the Court of Appeals has] recognized, first, that the General Assembly may act pursuant to its police or other legitimate power to aid the courts in the performance of their judicial functions[.]").

Legislation that imposes DOIT-controlled cybersecurity training or reporting requirements on the Judiciary exceeds the permissible "limited exertion of legislative authority . . . to aid the courts in the performance of their judicial function." *Id.* at 699. Instead, the proposed legislation "dilutes the fundamental authority and responsibility vested in the judiciary to carry out its constitutionally required function." *Id.* Moreover, these bills far exceed the requirements of any existing statute by attempting to infringe on the Judicial Branch's administrative authority over its own information technology practices. Specifically, these bills seek to modify and extend to the Judiciary provisions of Title 10, Subtitle 13 of the State Government Article and Title 3A of the State Finance and Procurement Article, both of which clearly do not apply to the Judicial Branch.

The efficient administration of justice in Maryland requires various information technology systems in courtrooms, clerks' offices, and Judiciary administrative offices. The Judiciary must maintain administrative control over its information technology practices, including decisions about network and data security, in order to carry out the judicial function. The Judiciary already has its own information technology department (Judicial Information Services, "JIS") which has thorough cybersecurity systems and safeguards in place, including quarterly cybersecurity training for all Judiciary employees. In addition, JIS already regularly collaborates with DOIT as to network and data security.

Accordingly, I believe that these bills impermissibly infringe upon the authority constitutionally vested in the Judicial Branch as a co-equal branch of State government.

Very truly yours,

Joseph M. Getty
Chief Judge
Court of Appeals of Maryland