JacksonSB107Testimony.pdf
Uploaded by: Michael Jackson
Position: FAV

MICHAEL A. JACKSON
Legislative District 27
Calvert, Charles and
Prince George's Counties

Budget and Taxation Committee
Subcommittees
Pensions
Public Safety, Transportation, and
Environment

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
Miller Senate Office Building
11 Bladen Street, Suite 3 West
Annapolis, Maryland 21401
410-841-3700 · 301-858-3700
800-492-7122 *Ext.* 3700
Michael.Jackson@senate.state.md.us

District Office
250 Merrimac Court
Prince Frederick, Maryland 20678

TESTIMONY - SENATE BILL 107

STATE GOVERNMENT – STATE AND LOCAL GOVERNMENT EMPLOYEES AND CONTRACTORS – CYBERSECURITY TRAINING

EDUCATION, HEALTH, & ENVIRONMENTAL AFFAIRS COMMITTEE

MARCH 3, 2022

Chair Pinsky, Vice Chair Kagan, and Member of the Education, Health, and Environmental Affairs Committee:

Senate Bill 107 is a straight-forward bill that simply establishes a Cybersecurity Awareness and Training Program for State employees and contractors. Under the legislation, the Maryland Cybersecurity Coordinating Council, in corroboration with the State Chief Information Security Officer, would be tasked with creating the program for State employees consisting of periodic cybersecurity training activities. The State Chief Information Security Officer would also be required to approve and audit certified training courses for contractors accessing State or local government computer systems and databases.

Because of the sensitive nature of the information with which government employees and contractors deal, it's absolutely imperative that we take every precaution necessary to guard the information of Maryland citizens. With identity theft and related-crimes at an all-time high, the program created by this legislation would provide a needed and critical protection for all of those with information in State databases.

For the reasons listed above, I ask for a favorable report of Senate Bill 107.

CAMI Written Testimony - SB 107.pdf
Uploaded by: Tasha Cornish
Position: FAV

CYBERSECURITY
ASSOCIATION OF MARYLAND, INC.

FAVORABLE

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

SENATE BILL 107
State Government - State and Local Government Employees and Contractors - Cybersecurity Training

Tasha Cornish on behalf of the
Cybersecurity Association of Maryland, Inc.

POSITION: FAVORABLE

March 2, 2022

Chairman Pinksy, Vice Chairwoman Kagan, and Members of this Committee, thank you for the opportunity to submit testimony in support of Senate Bill 107.

Human error is a leading entry point for cybersecurity vulnerabilities, but a well-trained and cyber aware workforce can also be our most powerful tool. By implementing evidence-based cybersecurity awareness programs across government entities, employees can recognize security threats and know how to properly respond and escalate issues. When awareness training is offered on an ongoing basis, it builds a security aware culture and employees understand their role in keeping our State and Local systems secure. By centralizing an approval process for the cybersecurity awareness training within the Maryland Cybersecurity Coordinating Council, this Bill establishes a foundation for quality control and accountability, while also allowing space for some local customization when needed.

This is a critical step in reducing cybersecurity incidents and protecting our systems and data. Our organization urges a favorable report. Thank you again for the opportunity to testify.

Cybersecurity Association of Maryland, Inc. (CAMI)
1215 E Fort Ave Suite 203, Baltimore, MD 21230
443-376-8667 www.MDcyber.com

SB 107_HB 5 - Amendment.pdf
Uploaded by: Bryson Popham
Position: FWA

By:

AMENDMENTS TO HOUSE BILL 5
(First Reading File Copy)

Amendment No. 1:
On page 4, after line 15 add:

"**(III) A CYBERSECURITY TRAINING PROGRAM DEVELOPED BY A CONTRACTOR MAY BE CONSIDERED FOR CERTIFICATION UNDER THIS SUBSECTION"**

Rationale:
This clarifies that a contractor with a robust cybersecurity training program that meets or exceeds standards adopted under this Subtitle may be considered and approved by the State Chief Information Security Officer.

SB 107_T.ROWE PRICE_FWA.pdf
Uploaded by: Bryson Popham
Position: FWA

Bryson F. Popham, P.A.

Bryson F. Popham, Esq.

191 Main Street
Suite 310
Annapolis, MD 21401
www.papalaw.com

410-268-6871 (Telephone)
443-458-0444 (Facsimile)

March 3, 2022

The Honorable Senator Paul G. Pinsky, Chairman
Senate Education, Health, and Environmental Affairs Committee
2 West, Miller Senate Office Building
Annapolis, Maryland 21401

RE: Senate Bill 107 - State Government - State and Local Government Employees and Contractors - Cybersecurity Training FWA

Dear Chairman Pinsky and Members of the Committee,

I am writing to you on behalf of my client, T. Rowe Price Group, Inc. T. Rowe Price is a global financial services company headquartered in Baltimore, Maryland, with an additional campus in Owings Mills, Maryland, and other offices in the United States and abroad.

As a worldwide financial services company, the subject of cybersecurity is of paramount importance to T. Rowe Price. The Committee may know that, in addition to its many individual, corporate and government clients, T. Rowe manages the 529 College Savings Plan for Maryland. Protecting the assets of those who entrust those assets to T. Rowe Price is vitally important.

T. Rowe has a world class cybersecurity training program, and it welcomes this measure by the Maryland legislature to instill appropriate standards for cybersecurity training. The Company is confident in its ability to meet these standards, and believes that its own cybersecurity training would meet or exceed the Maryland requirements.

Senate Bill 107 sets forth a procedure for certification of cybersecurity training by the State Chief Information Security Officer, set forth on page 4, lines 10 through 15 of Senate Bill 107. T. Rowe proposes a clarifying amendment to that language that expressly authorizes this officer to consider and approve a training program by a contractor for certification. We hope and believe this meets the legislative intent of the bill.

T. Rowe respectfully requests the Committee to issue a favorable report on Senate Bill 107, with the requested attached amendment.

Very truly yours,

Bryson F. Popham

cc: The Honorable Carol L. Krimm
The Honorable Samuel I. Rosenberg
Karen Nash-Goetz, Esq.

SB0107-EHE_MACo_SWA.pdf
Uploaded by: Dominic Butchko
Position: FWA

MARYLAND Association of COUNTIES

Senate Bill 107

State Government - State and Local Government Employees and Contractors - Cybersecurity Training

MACo Position: **SUPPORT WITH AMENDMENTS**

To: Education, Health, and Environmental Affairs Committee

Date: March 3, 2022

From: Dominic J. Butchko

The Maryland Association of Counties (MACo) **SUPPORTS** SB 107 **WITH AMENDMENTS.** As currently written, this bill preempts county government's decisions regarding cybersecurity trainings for employees. Amendments can bring the bill's approach closer to a mutual framework for collaboration – to advance these goals more flexibly.

County governments are established and complex employers and entities – something as critical as cybersecurity cannot be driven by one-size-fits-all policies. SB 107 overrides local autonomy on how best to implement cybersecurity training programs for their employees.

Counties all currently have thorough local cybersecurity training. Most of Maryland's jurisdictions use the program "KnowB4" for cybersecurity training – which could be mandated to change should this bill be enacted. **After speaking with the bill sponsor, MACo agrees with their intent, which would be to provide additional resources to local governments for cybersecurity training and not mandate what those trainings should be.**

MACo asks the committee to use the following points to guide amendments and best meet the common goals under this initiative:

1.) The State can set minimum standards for cybersecurity training that counties can exceed;
2.) The State can develop training courses that meet minimum standards set by the State, and counties may opt to use those trainings free of charge;
3.) The State will provide additional financial resources to help pay for cybersecurity trainings not provided by the State; and
4.) Counties may retain their current cybersecurity training providers and will not be required to use providers determined by the State.

MACo does not oppose the idea of increased cybersecurity training, but as written, SB 107 oversteps the boundaries of local autonomy and does not allow for any county input in the process. Accordingly, MACo urges a **FAVORABLE WITH AMENDMENTS** report on SB 107.

SB 107.State and Local Cyber Training.pdf
Uploaded by: John Woolums
Position: FWA

MABE
MARYLAND ASSOCIATION OF BOARDS OF EDUCATION

621 Ridgely Avenue, Suite 300, Annapolis, Maryland 21401
410-841-5414 · 800-841-8197 · Fax: 410-841-6580 · MABE.org

BILL: **Senate Bill 107**
TITLE: **State Government - State and Local Government Employees and Contractors - Cybersecurity Training**
DATE: **March 3, 2022**
POSITION: **SUPPORT WITH AMENDMENTS**
COMMITTEE: **Education, Health, and Environmental Affairs**
CONTACT: **John R. Woolums, Esq.**

The Maryland Association of Boards of Education (MABE) supports Senate Bill 107 to establish the State Cybersecurity Awareness and Training Program with amendments to address concerns regarding local decision-making as to the administration of cyber security training and other issues.

MABE, on behalf of all local boards of education, certainly appreciates and supports the need for increased investments and opportunities for state and local employees to participate in cyber security training. School systems throughout the nation, and in Maryland, have experienced first-hand the dire consequences of cyberattacks. These experiences are having significant impacts on school system budgets in areas including technology, staffing, professional development, insurance, and risk management. Senate Bill 107 would meaningfully enhance the State's approach to providing the resources needed to ensure continuous improvement in cybersecurity across all state agencies and among Maryland's diverse array of local governments and school systems.

One provision of the bill, however, raises a concern regarding the breadth and scope of the mandated trainings. Specifically, the bill includes a mandate to require each employee whose job duties include accessing a computer system or data base to complete at least four trainings each year. MABE agrees that such trainings are needed for certain employees and is requesting an amendment to clarify that the mandate would apply to local employees identified by the local government or school system. Local boards believe this amendment would allow for appropriate local discretion to define the scope and application of the training mandate. Similarly, given the potential for an enormous number of employees being required to participate in annual training, MABE requests local discretion on the number of distinct trainings as well.

MABE looks forward to the Cyber Security Council's development of standards for the Cybersecurity Awareness and Training Program, including the certification of specific training programs, and to ongoing collaboration with the State to build a robust and resilient cybersecurity bulwark against cyberattacks and their disruptive, costly, and at times devastating impacts on Maryland's public school systems.

For these reasons, MABE requests a favorable report on Senate Bill 107, with the amendments described above.

SB 107_FWA_MML.pdf
Uploaded by: Justin Fiore
Position: FWA

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 107 – State Government – State and Local Government Employees and Contractors – Cybersecurity Training

Position: Support with Amendment

Reason for Position:

The Maryland Municipal League supports SB 107 with amendments. As introduced, the bill mandates local government employees to complete State-approved cybersecurity trainings at least four times per year.

The League appreciates the sponsors intent to create a training program for local governments to better protect resident data and our systems. In conversations with the sponsor, we understand the intent was even to make these programs available for free. This would be a great example of the type of resources MML has advocated for the past several sessions.

We do believe, however, that the bill needs clarity to ensure this program would be free to municipal employees. Our members would also appreciate amendments to ensure the content of the trainings developed by the MCCC are applicable to local government and be created in consultation with local government. Further, in cases where municipalities already retain a vendor to provide these functions, we would ask that it fulfill the requirements of the bill as to not be duplicative. Still yet, cities and towns would request the discretion to set the schedules for trainings as it relates to the needs of their employees.

Therefore, the League respectfully requests time to continue working with the sponsor and committee on amendments and provide SB 107 with a favorable report.

FOR MORE INFORMATION CONTACT:

1212 West Street, Annapolis, Maryland 21401

410-268-5514 | 800-492-7121 | FAX: 410-268-7004 | www.mdmunicipal.org

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

SB107_USM_FWA_Cather.pdf
Uploaded by: Mark Cather
Position: FWA

UNIVERSITY SYSTEM of MARYLAND

SENATE EDUCATION, HEALTH, AND ENVIRONMENTAL AFFAIRS COMMITTEE
Senate Bill 107
State Government – State and Local Government Employees and Contractors – Cybersecurity Training
March 3, 2022
Favorable with Amendment

Delegate Pinsky, Vice Chair Kagan and committee members, thank you for the opportunity to share our thoughts on Senate Bill 107. The bill requires quarterly cybersecurity training developed and prescribed by the Maryland Cybersecurity Coordinating Council.

The University System of Maryland (USM) agrees wholeheartedly that IT security training is an integral part of securing State and university IT systems. The USM has developed cybersecurity policies approved by the Board of Regents appropriate for higher education institutions that are in keeping with this bill and statute requiring USM to remain functionally compatible with State of Maryland IT policy, which requires annual training. Included in USM's IT Security Standards, to which all USM institutions are audited by Maryland Office of Legislative Audits, USM Internal Audits and 3rd party auditors, is the requirement to develop and execute a cybersecurity training and awareness program.

Senate Bill 107 would require that USM institutions accommodate the quarterly training in addition to the more tailored trainings being done institutionally that are more specifically geared to the needs of higher education. It is likely that USM institutions would need to hire additional staff to administer the quarterly training requirement. In addition, the bill has the training being developed and set by the Maryland Cybersecurity Coordinating Council (MCCC). That council is a part of the executive branch, and public higher education has not typically fallen under that council.

The USM respectfully requests an amendment to be exempted from the requirements called for under Senate Bill 107.

Thank you for allowing the USM to share these concerns regarding Senate Bill 107.

About the University System of Maryland

The University System of Maryland (USM)—one system made up of 12 institutions, three regional centers, and a central office—awards 8 out of every 10 bachelor's degrees in the State of Maryland. The USM is governed by a Board of Regents, comprised of 21 members from diverse professional and personal backgrounds. The chancellor, Dr. Jay Perman, oversees and manages the operations of USM. However, each constituent institution is run by its own president who has authority over that university. Each of USM's 12 institutions has a distinct and unique approach to the mission of educating students and promoting the economic, intellectual, and cultural growth of its surrounding community. These institutions are located throughout the state, from western Maryland to the Eastern Shore, with the flagship campus in the Washington suburbs. The USM includes Historically Black Colleges and Universities, comprehensive institutions, research universities, and the country's largest public online institution.

USM Office of Government Relations - Patrick Hogan: phogan@usmd.edu

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

SB 107 State Government - State and Local Governme

Uploaded by: Anna Yates

Position: INFO

ST MARY'S COLLEGE of MARYLAND
The National Public Honors College

OFFICE OF THE PRESIDENT
47645 College Drive
St. Mary's City, MD 20686

www.smcm.edu
TEL: 240-895-4410
FAX: 240-895-4462

Senate Bill 107
State Government - State and Local Government Employees and Contractors - Cybersecurity Training
Senate Education, Health, and Environmental Affairs Committee
March 3, 2022

Letter of Information

Chair Pinsky, Vice Chair Kagan, and Members of the Committee,

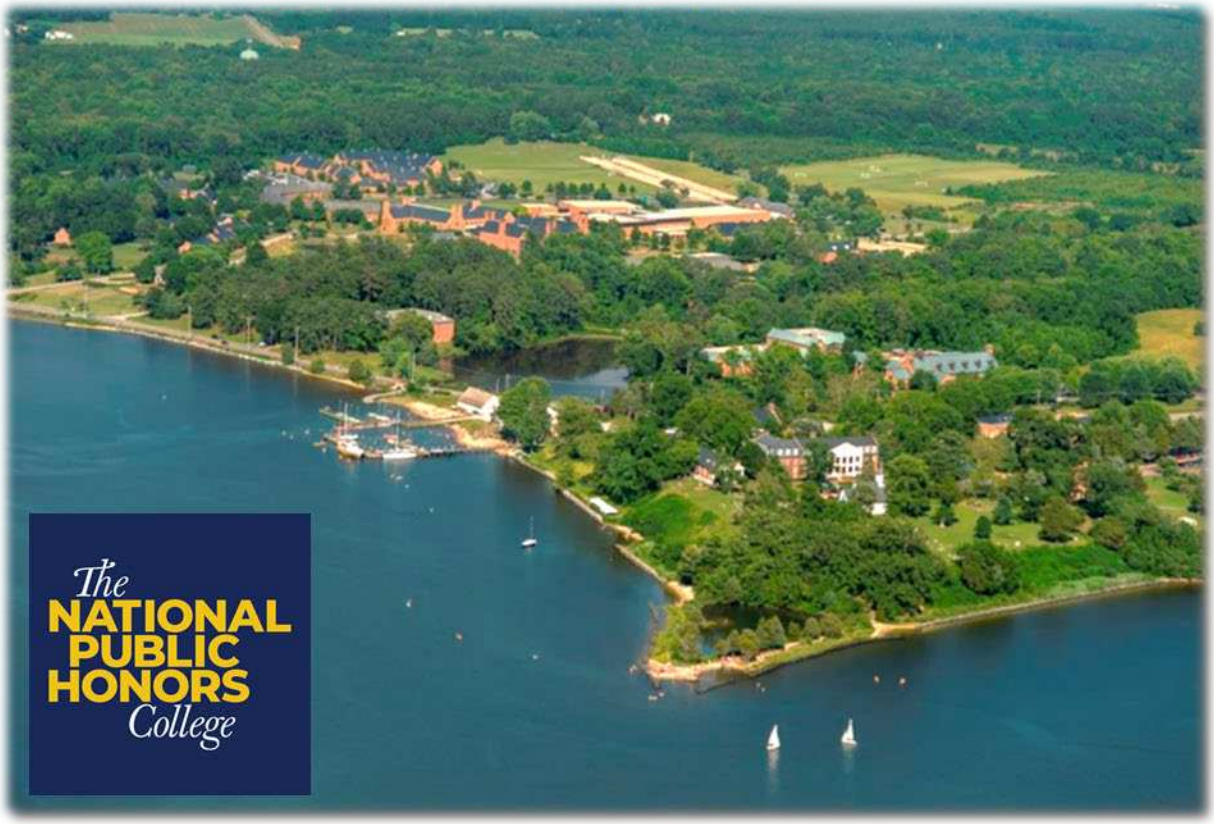
Thank you for the opportunity to share our thoughts on Senate Bill 107 - State and Local Government Employees and Contractors - Cybersecurity Training. St. Mary's College of Maryland is currently engaged in the implementation of a Cybersecurity Awareness and Training Program for students, faculty, and staff, including contractors. The certification training is expected to be complete in May 2022. The training provided by the College, which meets the requirements and guidance within the State of Maryland Treasurer Office's cybersecurity insurance policy, is encompassing, thorough, and relevant to the needs of higher education.

While all students, faculty, staff, and contractors will receive cybersecurity training, those whose positions require access to federal, state, and local government systems will receive specialized training, based on their roles and responsibilities, that is specific to their area and the information they share or access. The College's Assistant Vice-President of Information Technology/Chief Information Officer is responsible for determining both the general and specific training needs of each individual on campus and ensuring that the required training is completed.

Senate Bill 107 requires a significant amount of additional training, management, and oversight, for which the College would need to hire an Information Technology Security Officer at a cost of $150K plus benefits annually. Further, the additional and frequent interaction with the Department of Information Technology through the audit and verification processes required by the Bill would result in additional costs to the College, which are unknown at this time.

Thank you for your continued support of St. Mary's College of Maryland.

Tuajuanda C. Jordan, Ph.D.
President



U.S. NEWS & WORLD REPORT
BEST COLLEGES 2022
LIBERAL ARTS COLLEGES

KIPLINGER'S
BEST COLLEGE VALUE 2019

MONEY
BEST COLLEGES 2020

COLLEGES OF DISTINCTION
PUBLIC
2020 2021

THE PRINCETON REVIEW
387 BEST COLLEGES 2022

FEATURED IN 2021
FISKE GUIDE TO COLLEGES