JACKSONSB873TESTIMONY.pdf
Uploaded by: Jackson, Michael
Position: FAV

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

Judicial Proceedings Committee

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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

TESTIMONY - SENATE BILL 873

DEPARTMENT OF INFORMATION TECHNOLOGY – STATE AND LOCAL GOVERNMENT EMPLOYEES AND CONTRACTORS – CYBERSECURITY TRAINING

MARCH 2, 2021

Chair Pinsky, Vice Chair Kagan and Committee Members:

Senate Bill 873 is a piece of legislation that implements one of the chief recommendations of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology in creating a statewide cybersecurity training apparatus.

The bill would require the Department of Information Technology (in coordination with the Maryland Cybersecurity Council) to develop criterion for the certification of varied cybersecurity training programs used by state and local government employees. The certification criteria would focus on forming information security habits to protect information resources, personal information, and records. The bill would additionally mandate the Department of Information Technology to certify at least twenty cybersecurity training programs and to maintain a list of all certified programs.

The legislation would also require corresponding state and local government employees, as well as certified contractors, to complete said training programs and require their government units to report the completion of employee training to the Department of Information Technology. To ensure compliance, the bill includes audit requirements at both the State and local unit level.

As the former House Chair of the Joint Committee on Cybersecurity, Information Technology, and Biotechnology, I became acutely aware of the necessity of improving cybersecurity throughout state and local government. This piece of legislation is a significant step forward in achieving that aim and ensuring the safety of vital information.

For the reasons listed above, I ask for a favorable report of Senate Bill 873.

SB 873 - HB 1129 - T.ROWE PRICE - FWA.pdf
Uploaded by: Popham, Bryson
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)

February 25, 2021

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

RE: Senate Bill 873 - Department of Information Technology - State and Local Government Employees and Contractors - Cybersecurity Training - FWA

Dear Chairman Pinsky, Senator Jackson and Members of the Committee,

On behalf of my client, T. Rowe Price Group, Inc., I am writing to express our support for Senate Bill 873, with amendments. T. Rowe Price is a global financial services company headquartered in Baltimore, Maryland, with an additional campus in Owings Mills Maryland.

The legislation requires the Department of Information Technology, in coordination with the Maryland Cybersecurity Council, to develop criteria for, and to certify, cybersecurity training programs for use across state and local government in Maryland. Personnel in state and local government with access to government computer systems or databases would be required to complete an approved training program annually. The certification requirements under Senate Bill 873 include certification of training programs to be used by personnel of private businesses that contract with government agencies, where the contractor has access to the computer systems or databases of a government unit. Furthermore, Senate Bill 873 requires the Department of Information Technology to approve at least one certified program for outside contractors. We note that, among other things, the bill requires that the Department shall certify at least 20 cybersecurity training programs for use by governmental employees and update the certification list annually.

T. Rowe Price has a long history of protecting confidential information on behalf of its customers and others. For many years, there has been an annual requirement for its personnel to have at least one (and depending on an employee's area, more than one) cybersecurity training. Training programs are sometimes developed internally, and other times may rely on a vendor-supplied module with minimal customization. They are evaluated and refreshed as needed to keep up with the developing threat landscape. T. Rowe Price believes that Maryland law should permit contractors to utilize their own training programs that are designed to be consistent with the goals stated in the bill for the Department to use in assessing cybersecurity training programs (e.g., inclusion of activities, case studies, hypothetical situation, and other methods that focus on forming information security habits, detecting and reporting security threats, etc.).

It is our understanding that the Department will not take a position on the bill, and they suggested that we approach Senator Jackson or Delegate Krimm with our request.

Accordingly, T. Rowe Price respectfully requests an opportunity to work with Senator Jackson and Committee Counsel on amendment language that would permit a contractor to use its own training program under certain circumstances. Those circumstances would include a requirement that the contractor’s training program is consistent with the criteria

stated in the bill for cybersecurity training programs. If the contractor's training program fails to meet those criteria, the Department could simply require the contractor to use a training program on the Department's approved list.

The Committee may wish to add other conditions, such as an additional requirement that a contractor relying on its own training program must provide a copy of the program to either the Department or the particular government agency involved. We respectfully submit that this is a common sense approach that will streamline the training process without sacrificing quality in the established standards.

Thank you for your consideration of this request.

Very truly yours,

Bryson Popham, Esq.

cc: The Honorable Michael A. Jackson - michael.jackson@senate.state.md.us
The Honorable Carol L. Krimm - Carol.Krimm@house.state.md.us

SB 873_UNF_MML.pdf
Uploaded by: Fiore, Justin
Position: UNF

Maryland Municipal League

The Association of Maryland's Cities and Towns

TESTIMONY

March 2, 2021

Committee: Senate Education, Health, and Environmental Affairs

Bill: SB 873 - Department of Information Technology - State and Local Government Employees and Contractors - Cybersecurity Training

Position: Oppose

Reason for Position:

The Maryland Municipal League opposes SB 873 which sets mandatory training for certain municipal employees and requires periodic audits of the training program compliance.

While MML recognizes the importance of mitigating risks of a cyber attack on local governments, particularly in this era of expanded telework, the training mandate for all municipal employees that interact with the government computer systems infringes on local authority as employers to govern their business. This mandate, which also applies to contractors, is overbroad and may in many instances be unnecessary in some circumstances and duplicative in others.

Secondly, the mandatory periodic audits may put a fiscal strain on some municipalities. In many instances, audits come with a significant price tag and may not be an appropriate use of funds if, for instance, a municipality on has a few employees.

For these reasons we therefore respectfully request that the committee provide an unfavorable report on SB 873.

FOR MORE INFORMATION CONTACT:

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

SB0873-EHE_MACo_OPP.pdf
Uploaded by: Jabin, Drew
Position: UNF

MARYLAND Association of COUNTIES

Senate Bill 873

Department of Information Technology - State and Local Government Employees and Contractors - Cybersecurity Training

MACo Position: **OPPOSE**

To: Education, Health, and Environmental Affairs Committee

Date: March 2, 2021

From: Drew Jabin

The Maryland Association of Counties (MACo) **OPPOSES** SB 873. While well-intentioned, this bill would place a detailed mandate on county governments to carry out new state policy and implement State-mandated cybersecurity training programs.

County governments are established and complex employers and entities – and are not truly in need of the degree of hands-on requirements that SB 873 envisions. As a rule, MACo resists state policies that result in costly or burdensome local implementation. SB 873 overrides local autonomy on how best to implement cybersecurity training programs.

Counties all currently have thorough local cybersecurity training and are already meeting the spirit of this legislation. While counties do not oppose the general intention of the State providing cybersecurity guidance and best practices, SB 873 concerningly lacks any hint of local input. Most of Maryland's jurisdictions use the program "KnowB4" for cybersecurity training – which could be mandated to change as the state Department of Information Technology, in coordination with the Maryland Cybersecurity Council, is tasked with determining what programs will fill the 20 slots allotted under this bill without appropriate deference to what tools are already successful locally.

Again, MACo does not oppose the idea of increased cybersecurity training, but SB 873 oversteps the boundaries of local autonomy and does not allow for any county input in the process. Accordingly, MACo **OPPOSES** SB 873 and requests an **UNFAVORABLE** report.

169 Conduit Street, Annapolis, MD 21401
410.269.0043 BALT/ANNAP ◆ 301.261.1140 WASH DC ◆ 410.268.1775 FAX
www.mdcounties.org