SB390_MDOD_FAV.pdf
Uploaded by: Elizabeth Hall
Position: FAV

Carol A. Beatty, Secretary
Christian J. Miele, Deputy Secretary

Larry Hogan, Governor
Boyd K. Rutherford, Lt. Governor

Maryland
DEPARTMENT OF DISABILITIES

DATE: March 3, 2022
BILL: Senate Bill 390
COMMITTEE: Senate Education, Health, and Environmental Affairs Committee
POSITION: Favorable, Letter of Support

Dear Chair Pinsky:

The Maryland Department of Disabilities (MDOD) is pleased to provide this letter in support of Senate Bill 390 Government - Information Technology - Cybersecurity departmental legislation requested by the Department of Information Technology.

The purpose of SB390 is to codify provisions such as the Cybersecurity Coordinating Council. MDOD oversees the IT Accessibility Initiative, a team charged with improving policies and practices in state IT development and procurement for equal access to state agency information technology. Including MDOD on the council ensures that information technology (IT) accessibility is represented as a cornerstone of the State's Cybersecurity response as it develops strategies and policies for state government. The IT Accessibility Initiative team has developed ongoing inter-agency relationships focused on access across the state via evaluations of all state websites and state technology platforms, inter-agency consultations, procurement policy development and training, technical assistance focused on website and platform remediation, and ongoing, statewide IT accessibility training.

As the Cybersecurity Council seeks to establish strategies, policies, recommendations, and implement security requirements, the MDOD representative will consider the accessibility and access of these recommendations.

MDOD respectfully requests a favorable report on SB390.

If there are any questions, please contact MDOD's Director of Interagency Affairs, Elizabeth Hall, elizabeth.hall2@maryland.gov

Sincerely,

Carol A. Beatty

Carol A. Beatty, Secretary

SB 390_Governors Office_Support.pdf
Uploaded by: Erin Chase
Position: FAV

STATE OF MARYLAND
OFFICE OF THE GOVERNOR

LARRY HOGAN
GOVERNOR

STATE HOUSE
100 STATE CIRCLE
ANNAPOLIS, MARYLAND 21401-1925
410-974-3901
TOLL FREE 1-800-811-8336

TTY USERS CALL VIA MD RELAY

Senate Bill 390 State Government - Information Technology - Cybersecurity

Position: Support

Senate Education, Health, and Environmental Affairs Committee

March 3, 2022

Erin Chase, Deputy Legislative Officer, Office of the Governor

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

Senate Bill 390 will codify the Administration's executive order creating the Office of Security Management, State Chief Information Officer (SCISO), and the Maryland Cybersecurity Coordinating Council (MCCC), as well as provide the SCISO with additional authority to mitigate any cybersecurity threats impacting the state's network.

Understanding the constant emerging threat of cybersecurity incidents, in 2019 Governor Hogan signed Executive Order 01.01.2019.07, which formally established the Maryland Cyber Defense Initiative to strengthen the State's ability to manage the consequences of a cybersecurity incident. The Maryland Cyber Defense Initiative consists of three primary functions: the creation of the SCISO, Office of Security Management, and MCCC. The SCISO is a critically important position that provides cybersecurity advice, recommendations, and consultation to the governor, as well as responding to cyber threats and incidents. The Office of Security Management houses the SCISO and is responsible for the direction, coordination, and implementation of the overall cybersecurity strategy and policy for the Executive Branch. The MCCC consists of senior level staff members from several cabinet agencies and works closely with the SCISO to provide advice and recommendations regarding the strategy and implementation of cybersecurity initiatives and recommendations, and building and sustaining the State's capability to identify, mitigate, and detect cybersecurity risk, and respond to and recover from cybersecurity-related incidents. The initiative is key to strengthening the state's cyber posture. The state is ultimately accountable and responsible for the protection of this private and sensitive information, and it is crucial that our statute accurately reflects that.

Additionally, the bill provides the SCISO with additional authority to take or direct actions to mitigate threats if there is risk to the state's network. State agencies are aware of the threat that bad actors play in cybersecurity incidents, but the SCISO needs to be equipped with the tools necessary to take decisive action to protect the state's assets if the situation arises.

To further strengthen the state's cybersecurity posture, the Fiscal Year 2023 budget includes funds to grow the cyber workforce and key investments in IT infrastructure. Some of the highlights include:

- $3 million for a new Center for Cybersecurity at the University of Maryland, Baltimore County (UMBC);
- $1 million over two years to establish the Maryland Institute for Innovative Computing at UMBC to accelerate innovation and develop a talent pipeline for state agencies in computing, especially cybersecurity, AI, and data science;
- $1 million for the Cybersecurity Public Service Scholarships, an increase of $860,000;
- $3.8 million for Cyber EARN, an increase of $1 million;
- $333.9 million for Major Information Technology Projects, which supports 44 projects to modernize legacy IT and make the state's infrastructure more secure;

- $10 million for cybersecurity assessments;
- $100 million in the Dedicated Purpose Account to protect and mitigate against cybersecurity incidents.

As we continue to bolster our state's position on issues relating to cybersecurity, Maryland must have a consistent and responsible law that establishes our cybersecurity policies. The Hogan administration understands that the State stores and processes a large volume of sensitive data and has a responsibility to its citizens and other data owners to protect the confidentiality, availability, and integrity of this data. Senate Bill 390 will ensure that these duties are enshrined in Maryland's statute.

For these reasons, the Administration respectfully requests a favorable report on Senate Bill 390.

SB0390 (HB0419) - FAV - State Government - Inform

Uploaded by: Landon Fahrig

Position: FAV

Maryland Energy Administration

Larry Hogan, Governor
Boyd K. Rutherford, Lt. Governor
Mary Beth Tung, Director

TO: Members, Senate Education, Health, and Environmental Affairs Committee
FROM: Mary Beth Tung – Director, MEA
SUBJECT: SB 390 (HB 419) - State Government - Information Technology - Cybersecurity
DATE: March 3, 2022

MEA POSITION: FAV

The Maryland Energy Administration (MEA) strongly supports this legislation that will establish the position of State Chief Information Security Officer and an Office of Security Management within the Department of Information Technology, as well as codify the Maryland Cybersecurity Coordinating Council (Council).

The need for continually evolving cybersecurity efforts is evidenced by events that often make front page headlines. One energy-related event was the May 2021 ransomware attack on Colonial Pipeline Company (Colonial), where the system temporarily suspended operations as a precautionary measure. Colonial supplies 45% of Maryland's total liquid fuel, including for both air and ground operations at Baltimore/Washington International Thurgood Marshall Airport as well as the ground vehicles for the Port of Baltimore. The affected regions, including Maryland, experienced higher prices at the pump, panic buying, and supply shortages. Stores that typically sell ~4,000 gallons of gasoline per day were selling ~4,000 gallon in a four-hour period. As a result, Maryland found itself in the unfortunate position of declaring a State of Emergency due to the major disruption to its fuel supply chain.

Fortunately, MEA, the Maryland Department of Transportation, and others, were able to mitigate the impacts of this event with coordination overseen by the Maryland Department of Emergency Management. The main reason that this energy disruption did not reach crisis level is because of the overall federal and state government response; stabilizing the energy supply lines and ensuring continuity of services.

The Colonial cyberattack was the largest attack on the U.S. energy system to date. Attacks such as this emphasize the new reality Maryland finds itself in, and highlights the pressing need to prioritize cybersecurity. **The new Chief Information Security Officer and Office of Security Management will undoubtedly improve the performance and function of state information systems with ever-evolving security enhancements.** MEA is particularly interested in the codification of the Council, which will provide the security related training and data sharing needed to minimize informational lag, promote more unified efforts, and facilitate interagency cooperation including that with federal agencies.

For these reasons, MEA kindly asks the committee to issue a **favorable report**.

SB390_DoIT_MichaelLeahy.pdf
Uploaded by: Patrick Mulford
Position: FAV

Date: March 3, 2022
Bill: Senate Bill 390 State Government - Information Technology - Cybersecurity
Position: Support

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

Dear Chairman Pinsky:

The Department of Information Technology (DoIT) supports Senate Bill 390 State Government - Information Technology - Cybersecurity. The purpose of this bill is to codify Governor Hogan's Executive Order 01.01.2019.07, which creates the position of State Chief Information Security Officer, the Office of Security Management and the Maryland Cybersecurity Coordinating Council (MCCC). These three entities are the driving force behind the Maryland Cyber Defense Initiative, which will strengthen the State's cybersecurity posture while also solidifying its ability to prevent when possible and then manage and minimize the consequences of a cybersecurity incident.

The State Chief Information Security Officer leads the Office of Security Management. The office, located within the Department of Information Technology, is responsible for the direction, coordination, and implementation of the overall cybersecurity strategy and policy for all State agencies in the Executive Branch.

The MCCC provides advice and recommendations regarding the implementation of cybersecurity initiatives and the building and sustaining of the capabilities necessary for the State to identify, protect, detect, respond, and recover from cybersecurity-related incidents. The MCCC is comprised of State officials representing numerous agencies and departments throughout the State. Having high ranking officials from numerous state agencies is a huge asset in working together to coordinate cybersecurity strategy throughout the whole executive branch.

The bill also requires the Legislative and Judicial branches to certify that they are in compliance with certain minimum security standards in reference to their connection to networkMaryland. This will help to ensure that they are not introducing, or exposing other entities to unneeded risk on the network.

In addition, the bill requires all executive branch agencies and units to submit a report to the Governor that contains:

1. an inventory of all information systems and applications used or maintained by the

agency or unit;
2. a full data inventory of the agency or unit;
3. a list of all cloud or statistical analysis system solutions used by the agency or unit; and
4. a list of all permanent and transient vendor interconnections that are in place.

This report will allow the State Chief Information Security Officer and the Office of Security Management to fully understand what data and systems are in each agency in the executive branch. An asset inventory is a logical beginning step for the Office of Security Management to minimize the agencies' cyber and privacy risks and serves as the foundation for creating a coordinated cybersecurity strategy across all agencies.

The Department of Information Technology does not expect there to be a financial impact related to this bill. The Department has already received and allocated funds for this legislation, as its requirements were implemented in 2019 pursuant to the Governor's Executive Order.

For these reasons, the Maryland Department of Information Technology respectfully requests a favorable report on Senate Bill 390.

Best,

Michael G. Leahy
Secretary
Department of Information Technology

CAMI Written Testimony - SB 390.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 390

State Government - Information Technology - Cybersecurity

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 390.

This bill moves Maryland forward in meaningful ways to have a strong cybersecurity posture by codifying current successes within the Maryland State government. By codifying the establishment of the Office of Security Management within the Department of Information Technology, the position of State Chief Information Security Officer, and the Maryland Cybersecurity Coordinating Council you will be adopting a best practice approach that will be difficult to change. The proposed alterations to the membership of the Council will strengthen this group that has proven itself effective and informative. Requiring each unit of the Legislative Branch or Judicial Branch of State government that uses a certain network to certify certain compliance to the Department by December 1 each year would give the State CISO the insight they need to protect our states systems and citizens effectively.

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

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