

2022 03 02 Motorola Written Testimony in Support o

Uploaded by: James Kaine

Position: FAV



PRODUCTS & SERVICES
CYBERSECURITY



FAVORABLE

March 2, 2022

The Honorable Paul G. Pinsky
Senate Committee on Education, Health, and Environmental Affairs
Miller Senate Office Building, 2 West Wing
11 Bladen St
Annapolis, MD 21401 - 1991

Dear Chairman Pinsky,

Motorola Solutions is a leading cybersecurity services provider committed to protecting our enterprise and public safety customers, and the communities they serve, from the constantly evolving threat landscape. We wish to affirm our support of SB754: Local Government Cybersecurity - Coordination and Operations (Local Cybersecurity Support Act of 2022), as a positive step forward in improving the defense of Maryland's critical networks and infrastructure.

Cyber threats are increasing in scope, scale, and complexity but most local governments lack the end-to-end cyber threat intelligence and defense capabilities required to adequately mitigate risk and ensure the continuity of public services. SB 754 acknowledges this reality and implements important measures to improve local government preparedness, including establishment of the Cybersecurity Fusion Center and the Local Cybersecurity Support Fund.

In accordance with SB 754, the fusion center will coordinate statewide cybersecurity as a central hub for information sharing across federal, state, and local entities as well as private sector organizations. It will play a critical role in supporting the "public-private operational collaboration" that the U.S. Cybersecurity & Infrastructure Security Agency's (CISA) Executive Director emphasized during recent testimony¹ before the U.S. Congress. Motorola Solutions looks forward to our collaboration with the fusion center as we continue to establish a Public Safety Information Sharing and Analysis Organization (ISAO), wholly dedicated to mitigating threats to public safety.

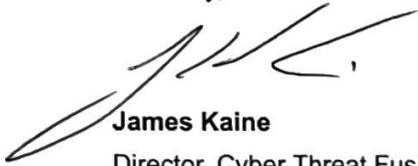
Another key provision within SB 754 establishes the Local Cybersecurity Support Fund to support local governments in the improvement of their cybersecurity preparedness. In addition to the purchase of new hardware and software, the provision provides local governments with funding for cybersecurity services from outside vendors including managed detection and response. Such cybersecurity services

¹ <https://oversight.house.gov/sites/democrats.oversight.house.gov/files/Wales%20Testimony.pdf>

will be critical given that all but the largest municipalities must focus their limited resources on core functions, including 9-1-1 and dispatch services, rather than in-house cybersecurity personnel that are in extremely short supply and capabilities that are too often cost prohibitive.

Motorola Solutions stands ready to support local governments across Maryland with world class cybersecurity services, coupled with our Public Safety ISAO, to advance the state's cybersecurity posture and preparedness. We applaud the General Assembly's focus on improving statewide cybersecurity through local government funding and empowerment, and we fully support passage of SB 754 as an important step moving forward.

Sincerely,

A handwritten signature in black ink, appearing to read 'JK', with a long, sweeping underline that extends to the left and then curves back to the right.

James Kaine

Director, Cyber Threat Fusion Center
Products & Services Cybersecurity

SB 754_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 754 – Local Government Cybersecurity – Coordination and Operations
(Local Cybersecurity Act of 2022)

Position: Support

Reason for Position:

The Maryland Municipal League supports SB 754, 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 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 754 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

1212 West Street, Annapolis, Maryland 21401

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

SB754 - Local Support Act of 2022 Sponsor Testimon

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



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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Sponsor Testimony - SB754 - The Local Cybersecurity Support Act of 2022

March 3, 2022

Thank you Chair, Vice Chair, and members of the committee for your consideration of SB754 - The Local Cybersecurity Support Act of 2022 - which leverages state resources to provide financial and technical assistance to local units of governments' efforts to increase their IT and 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 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). Unfortunately, the results confirm what we already know: no jurisdiction, regardless of its size, is immune to cyberattacks. In Maryland alone, large jurisdictions like Baltimore County have spent nearly \$8M to recover from attacks against their school systems, and small municipalities like Leonardtown and North Beach have been crippled by ransomware attacks.

Thankfully, our research revealed a number of possible resolutions to this threat, and SB754 is informed by those recommendations:


- First, it leverages the state's resources to codify and fully fund the Cyber Preparedness Unit within the Maryland Department of Emergency Management. This Unit is currently entirely funded by a 2-year federal grant and is working in collaboration with the State Chief Information Security Officer to support local government's development of vulnerability assessments and cyber preparedness/response plans. It would also serve as a point of contact for local governments to notify the state and mobilize relevant agencies if they are the victim of a cyberattack.
- Second, it establishes a Local Cybersecurity Support Fund to provide financial assistance for cyber preparedness efforts. This could include upgrading current devices, purchasing new software, or paying for cybersecurity training, but the language has also been amended to provide for increased flexibility to meet our county or municipal needs. This

also ensures that we're able to reduce disparities between larger, wealthy jurisdictions and smaller, low-income jurisdictions. This fund is also intended to serve as a local match for the State & Local Cybersecurity Grant program in the recently passed federal Infrastructure bill.

- Finally, it codifies the forthcoming Information and Analysis Center (ISAC) within the Department of Information Technology and in partnership with UMBC's Institute for Innovative Computing to coordinate and disseminate information on threats, resources, or responses to cybersecurity incidents.

In our digital age, it is not enough for the state to simply protect itself: vulnerabilities at the local level pose just as much a threat to our citizens' data as those at the state level. Our local governments are eager to address these vulnerabilities, but limited funding and staff present a significant obstacle. SB754 provides three distinct solutions to these problems by leveraging the state's resources, and for those reasons, **I respectfully request a favorable report from the committee.**

Sincerely,

A handwritten signature in cursive script that reads "Katie Fry Hester".

Senator Katie Fry Hester
Howard and Carroll Counties

Yelin Testimony - SB754 2022.pdf

Uploaded by: Ben Yelin

Position: FWA

TESTIMONY IN SUPPORT OF SB 754

LOCAL GOVERNMENT CYBERSECURITY - COORDINATION AND OPERATIONS (LOCAL CYBERSECURITY SUPPORT ACT OF 2022)

EDUCATION, HEALTH AND ENVIRONMENTAL AFFAIRS (EHE) COMMITTEE

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 754.

My name is Ben Yelin, and I am the Program Director for Public Policy & External Affairs at the University of Maryland Center for Health and Homeland Security, and an adjunct Professor at the University of Maryland Francis King Carey School of Law. This past year, I had the honor of serving as the co-chair of the Maryland Cybersecurity Council's ad hoc committee on State and Local Cybersecurity. We undertook a comprehensive study during the interim period to look at key issues in cybersecurity governance, state agency cybersecurity, and the cybersecurity posture of units of local government. The members of the ad hoc committee were proud to release this report at the end of last year and are grateful that many of its recommendations are being reflected in pieces of legislation before us today.

We are all familiar with the damage wrought by cyber-attacks on our local governments, such as the ransomware attack in Baltimore City that cost over \$18 million in system restoration and delayed or lost revenue, the 2021 attack on the Baltimore County school system and the Kaseya cyberattack that affected some of our smaller jurisdictions, including Leonardtown, MD. To better prepare for, mitigate, respond to, and recover from cyber-attacks in the future, Maryland needs to leverage the expertise of our state agencies to coordinate preparedness and response activities, and to provide financial assistance where needed.

Our study highlighted some of the vulnerabilities and preparedness gaps at the local level. Though counties, school districts, local emergency management departments and other units of local governments are making good faith efforts to improve their cybersecurity posture, a large portion of these agencies have still not completed vulnerability assessments, do not have consequence management plans, and do not have adequate staffing resources to address the current threat landscape. We heard in focus groups with representatives from County IT departments and representatives from local school districts that they could use the state's resources, particularly the Maryland Department of Emergency Management's expertise in resource coordination and a coalescer of preparedness materials, to improve its cyber readiness.

If passed, Senate Bill 754, as amended, would accomplish these goals. First, the bill would codify the existing Cyber Preparedness Unit in the Maryland Department of Emergency Management. This unit would be tasked with supporting local governments in its conducting vulnerabilities and risk assessments, maintain a database of cybersecurity resources, help units of local government adopt best preparedness practices as established by the State Chief Information Security Officer (SCISO), and support localities in obtaining resources needed for other preparedness activities. In addition, the bill establishes the local cybersecurity support fund, which would provide financial assistance to local

governments to enhance preparedness and to assist these units in obtaining federal cybersecurity resources.

I want to note that we worked closely with the Maryland Association of Counties and the Maryland Municipal League in crafting these recommendations. I am pleased that both organizations have expressed support for this bill with some amendments. We are fully supportive of these amendments, particularly removing the requirement that units of local governments must meet certain minimum security standards to obtain funds under the local cybersecurity fund. I am also pleased that in coordination with MDEM, and other stakeholders, we have suggested amendments to match the bill more closely to the agencies' capabilities and preexisting efforts.

I thank you for your attention today and your commitment to protect all Marylanders from the risks posed by cyber-attacks. I respectfully urge a favorable report, with amendments, on SB754.

SB0754-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

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.”

The Honorable Paul G. Pinsky
The Honorable Shane E. Pendergrass
March 2, 2022
Page 2

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.

The Honorable Paul G. Pinsky
The Honorable Shane E. Pendergrass
March 2, 2022
Page 3

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,

A handwritten signature in blue ink, appearing to read "J. M. Getty", is written over the typed name. The signature is stylized and includes a large checkmark-like flourish.

Joseph M. Getty
Chief Judge
Court of Appeals of Maryland