

**BaltimoreCounty\_FAV\_SB0069.pdf**

Uploaded by: Conner, Charles

Position: FAV



JOHN A. OLSZEWSKI, JR.  
*County Executive*

CHARLES R. CONNER III, ESQ.  
*Director of Government Affairs*

JOEL N. BELLER  
*Deputy Director of Government Affairs*

**BILL NO.:**           **SB 69**

**TITLE:**             Maryland Emergency Management Agency - Cybersecurity  
                                  Coordination and Operations Office – Establishment

**SPONSOR:**         Senator Hester

**COMMITTEE:**     Education, Health and Environmental Affairs

**POSITION:**       **SUPPORT**

**DATE:**             February 2, 2021

Baltimore County **SUPPORTS** Senate Bill 69 – Maryland Emergency Management Agency (MEMA) - Cybersecurity Coordination and Operations Office – Establishment. The legislation would establish a Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA).

When the Baltimore County Public School system suffered a ransomware attack, all of Baltimore County saw firsthand the devastation that can occur from vulnerabilities in cybersecurity. Swift action was required to get our students back in school, and it will take months of effort to fully recover our systems. Moving forward, it is essential that State and Local agencies undertake a coordinated effort to prevent and stem the effects of cybersecurity attacks in the future.

Senate Bill 69 would create a Cybersecurity Coordination and Operation Office within MEMA. This office would increase digital safety efforts by improving local, regional, and statewide cybersecurity readiness and response. They would also provide services to political subdivisions and school boards. This would help achieve cybersecurity best practices statewide. The office also would coordinate cybersecurity services throughout state agencies. This will keep the State’s digital information and technological services safe and secure from threat.

Accordingly, Baltimore County requests a **FAVORABLE** report on SB 69. For more information, please contact Chuck Conner, Director of Government Affairs, at [cconner@baltimorecountymd.gov](mailto:cconner@baltimorecountymd.gov).

**College Park City Council\_\_Robert Day\_\_Councilman\_\_**

Uploaded by: Day, Robert

Position: FAV

Mr. Robert Day  
Councilman, City of College Park, Maryland  
Member, Maryland Cybersecurity Council

Testimony in Support of

**SB 69**  
**Maryland Emergency Management Agency – Cybersecurity Coordination and Operations Office – Establishment**

Primary Sponsor: Senator Katie Fry Hester

Senate Education, Health, and Environmental Affairs Committee  
February 2, 2021

Chairman Pinsky, Vice Chairwoman Kagan, and Members of the Committee, thank you for the opportunity to testify in favor of SB 69.

My name is Robert Day, and I am councilmember for the City of College Park, a member of the Maryland Cybersecurity Council, and a Senior Management Officer with a Technology Development Firm, White Rook Technologies. I have been in the Information Technology and Network Security field for over 30 years.

The threat of ransomware attacks has increased over the last few years, with no sign of it slowing down. Since 2016, 48 states and the District of Columbia have had ransomware attacks wreak havoc on Police and Fire departments, phone systems email and many other services. In 2019 the known financial impact on state and local governments, healthcare providers, universities, colleges, and school districts are in excess of \$7.5 Billion. Last weekend, the City of Durham, North Carolina suffered a cyberattack which resulted in the City temporarily disabling all network access for Police, the 911 center, and the Fire Department phone services. This has hit close to home with the Baltimore attack costing the city at least \$18 million.

Certainly, there are cities and counties across our state that are meeting the growing challenges of security, modernization, innovation, and leading-edge applications, however far too many are living with serious deficiencies; both known and unknown. As a city council member for College Park, I would like to think that we are on the cutting edge and ahead of the curve when it comes to technology and network security... But from working in the field with a diversity of clients both Commercial and Federal, I know how fast things change, and how quickly sophisticated hackers adapt.

As an elected city official we must do our best to make sure to protect all of the valuable citizen information within our networks. A successful attack on our city would erode the public trust, would slow growth in our city, and affect the willingness of many to take a risk and try new endeavors, businesses or investments.

A 2019 University of Maryland, Baltimore County nationwide survey of cybersecurity in U.S. local governments stated that “Serious barriers to their practice of cybersecurity include a lack of cybersecurity preparedness within these governments and funding for it,” and that “Local governments as a whole do a poor job of managing their cybersecurity.” The issues identified included:

- Just over one-third did not know how frequently security incidents occurred, and nearly two-thirds did not know how often their systems were breached.
- Only a minority of local governments reported having a very good or excellent ability to detect, prevent, and recover from events that could adversely affect their systems.
- Fewer than half of the respondents said that they catalogued or counted attacks.

In some cases, governments failed to implement even the most basic of IT best practices. A key statement from this report:

*“Our research has shown that most American local governments do a poor job practicing cybersecurity. They must do better. And they can start by establishing a culture of cybersecurity throughout their organizations to best protect citizen information and maintain continuous service delivery.”*

*— Donald F. Norris, PhD, Professor Emeritus, UMBC;  
Laura Mateczun, JD, PhD student in Public Policy, UMBC.*

The state of Maryland must continue to be proactive in addressing and developing ways to be proactive to combat Cyber-attacks throughout our state. The National Governors Association report, “State Cyber Disruption Response Plans” brief warns:

*“Significant cyber incidents could... stretch the federal government’s ability to respond. In such a situation, states will need plans in place to ensure they are organized and prepared to respond without federal assistance.”*

Michael Garcia  
Senior Policy Analyst Homeland Security and  
Public Safety Division National Governors Association Center for Best Practices

Based on my experience working with IT infrastructure and Network and Cyber security, I strongly support SB 69 because it will boost the help needed to address the growing complexities of applying best practice’s, in planning and maintaining a strong Cybersecurity ecosystem throughout cities and local entities in our state. I agree that development of a Cybersecurity Coordination and Operations Office with reach throughout the state to help with assessments and implementation of best practices up and down the security stack will have immense impact.

I believe the objectives of this bill are necessary in developing a strong cybersecurity ecosystem within our state.

To the members of this committee, I thank you for your time and the opportunity to give testimony here today.

I encourage a favorable report of SB 69. Thank you for your consideration.

**MDGA\_Senator Hester\_FAV\_SB69.pdf**

Uploaded by: Hester, Katie

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

February 2nd, 2021

**Testimony in Support of SB69 - Maryland Emergency Management Agency -  
Cybersecurity Coordinations and Operations Office - Establishment**

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

Thank you for your consideration of Senate Bill 69. Last year, just before I presented this bill to this committee, the Federal Government's bipartisan US Cyberspace Solarium Commission issued its 182 page report. In it, the Commission highlighted a major takeaway of the current state of cybersecurity within the United States. The Commission states:

*"The U.S. government is currently not designed to act with the speed and agility necessary to defend the country in cyberspace... We must get faster and smarter, improving the government's ability to organize concurrent, continuous, and collaborative efforts to build resilience, [and] respond to cyber threats..."*

Over the past two years I have had the honor of serving as the co-chair of the Joint Committee on Cybersecurity, IT, and Biotechnology, and as a member of the Attorney General's Cybersecurity Council. Given my experience in these roles, it is with great concern that I must say, many of the issues identified by our counterparts in the U.S. Congress are not at all unique to the Federal government, and may in fact be more extensive at the State and local level. While actors around Maryland have been doing their best to address the grave risk that cybersecurity threats pose to critical infrastructure and systems, we still face large challenges in terms of coordinating resources effectively, making technical improvements to existing systems, sharing information and best practices across silos, and building the partnerships and knowledge base necessary to build resilience and response capacity to cybersecurity threats.

Senate Bill 69 seeks to address these issues by creating a Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency. The Office would be responsible for improving local, regional and statewide cybersecurity readiness by coordinating the activities of state and local entities as pertains to cybersecurity, and connecting these actors with the resources necessary to achieve their cybersecurity goals. This would include facilitating the exchange of information between political subdivisions, coordinating the provision of technical services, completing risk assessments, and developing up-to-date cyber disruption plans.

The Office would bring to bear a regional and organizational approach to managing the risks of cybersecurity threats, similar to those employed for natural disaster preparedness or the opioid crisis. In many ways, responding to and preparing for cybersecurity risks are very similar to natural disasters, in that they require continuous, collaborative effort, and that the proactive measures we take today will pay off the next time there is a cybersecurity incident. Cybersecurity threats can also vary greatly in scale and disruptive effect, making the need for a standing coordinating entity to build on pre-existing emergency response relationships and increase Maryland's cyber resilience capacity all the more urgent.

In 2019, Atlanta, Georgia; New Bedford, Massachusetts; New Orleans, Louisiana; Greenville, North Carolina; Pensacola, Florida; Wilmer, Texas; St. Lucie Florida; and our very own Baltimore City were victims of cybersecurity attacks, with costs in recovery and lost revenue stretching into the millions. In 2020 we have experienced a slew of cybersecurity attacks aimed at local governments and school systems, not the least of which is our very own Baltimore County Public Schools. With bad actors becoming more sophisticated, and the prevalence of cyber threats rising at almost every level of government and industry, the risk of a cyberattack is no longer "if," it's "when." This bill will make Maryland a leader in the nation, creating a first of its kind regional and cross-governmental structure capable of coordinating response and preparedness for cybersecurity threats in a variety of forms. I would also note for the committee's attention that this bill passed the Senate unanimously last session in this exact form. With this legislation we can adequately protect our constituents, and provide for a more effective defense of the State of Maryland. **I respectfully urge a favorable report for SB69.**

Sincerely,

A handwritten signature in black ink that reads "Katie Fry Hester". The signature is written in a cursive, slightly slanted style.

Senator Katie Fry Hester  
Carroll and Howard Counties



# **Yelin Testimony - SB69 2021.pdf**

Uploaded by: Yelin, Ben

Position: FAV

**TESTIMONY IN SUPPORT OF SB 69**

**“MARYLAND EMERGENCY MANAGEMENT AGENCY – CYBERSECURITY COORDINATION AND OPERATIONS OFFICE – ESTABLISHMENT”**

**EDUCATION, HEALTH AND ENVIRONMENTAL AFFAIRS (EHE) COMMITTEE**

**FEBRUARY 2, 2021**

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. I am speaking today on behalf of myself, the Center, and our Founder and Director Michael Greenberger. The Center provides comprehensive consulting services in the fields of emergency management and homeland security to governmental and institutional organizations, covering cybersecurity, emergency management, health security, and a variety of other services. The Center has developed, for example, cyber preparedness and response frameworks for Montgomery County and Prince George’s County. The Center also oversees new graduate specialties in cybersecurity and crisis management at the law school, where our Center has taught many courses in these areas, including Law and Policy of Cybersecurity and Law and Policy of Cyber Crimes. Both Professor Greenberger and Markus Rauschecker, the Center’s Cybersecurity Program Director, serve by appointment of the Maryland Attorney General on the Maryland Cybersecurity Council.

We are all familiar with the damage wrought by cyber attacks, such as the ransomware attack in Baltimore City that cost over \$18 million in system restoration and delayed or lost revenue, and the more recent attack on the Baltimore County school system. To better prepare for, mitigate, respond to, and recover from cyber attacks in the future, Maryland needs a coordinated infrastructure to integrate information, best practices, and resources across the state.

If passed, Senate Bill 1036 will do just that: establish a Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA). The Cybersecurity Coordination and Operations Office will improve local, regional, and statewide cybersecurity readiness and response. Because MEMA interfaces daily with state and local entities, it is perfectly situated to accomplish the mission set forth in SB1036:

- Assist in the development of local cybersecurity disruption plans;
- Coordinate with state and local entities on the implementation of cybersecurity best practices;
- Coordinate with local jurisdictions and agencies on the implementation of the Department of Information Technology’s Statewide Master Plan; and
- Work with the State Chief Information Security Officer and the Secretary of Information Technology to ensure that local jurisdictions and agencies have the resources they need for cybersecurity readiness and response.

This mission is essential to protecting the information technology infrastructure and functions of Maryland and its political subdivisions. I thank you for your attention to this threat and your commitment to protect all Marylanders from the risks posed by cyber attacks.

**SB0069 - LOI.pdf**

Uploaded by: Fahrig, Landon

Position: INFO



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:** SB0069 – Maryland Emergency Management Agency - Cybersecurity Coordination and Operations Office - Establishment  
**DATE:** February 2, 2021

---

**MEA POSITION: Letter of Information**

The purpose of the proposed legislation is to establish the Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA). The bill directs this new office to deliver and coordinate support services to include connecting multiple political subdivisions and agencies to share best practices to improve readiness, response, and implementation of cybersecurity best practices.

MEMA was an invaluable partner in the application leading to MEA and the State of Maryland being competitively selected by The National Governors Association to participate and evaluate lessons learned from GridEx V, a national-level electric grid cybersecurity exercise conducted by the North American Electric Reliability Corporation (NERC). This process was initiated in 2019, and it speaks to MEA’s understanding of the importance of this particular brand of planning.

The Cybersecurity Coordination and Operations Office could be a valuable tool in the continued efforts to defend the State from cybersecurity threats especially as it related to the energy grid. MEA works closely with MEMA as “State Coordinating Function 12” (Energy and Fuels representative) and plans, with or without this legislation, to utilize MEMA expertise for developing and maintaining its own planning and response procedures for cybersecurity events.

**2021-02-02 SB 69 (Letter of Information).pdf**

Uploaded by: Jung, Roy

Position: INFO

**BRIAN E. FROSH**  
*Attorney General*



**ELIZABETH F. HARRIS**  
*Chief Deputy Attorney General*

**CAROLYN QUATTROCKI**  
*Deputy Attorney General*

**STATE OF MARYLAND**  
**OFFICE OF THE ATTORNEY GENERAL**

FACSIMILE NO.

WRITER'S DIRECT DIAL NO.

410-576-6584

February 2, 2021

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

From: The Office of the Attorney General

Re: SB0069 – Maryland Emergency Management Agency - Cybersecurity Coordination and Operations Office - Establishment– **Letter of Information**

---

The Office of the Attorney General tenders this letter of information on SB 69.

Senate Bill 69 establishes and staffs a new Cyber Coordination and Operations Office (“CCOO”) within the Maryland Emergency Management Agency (“MEMA”) to prepare political subdivisions, school boards, and agencies against cybersecurity attacks. If enacted, the legislation would help these entities to develop cyber disruption plans, implement cyber best practices, coordinate with the Department of Information and Technology (“DoIT”) on the implementation of the State Master Plan, and connect these entities with resources in consultation with DoIT. Also, SB 69 instructs the CCOO to provide technical assistance to these entities, provide risk assessments, develop score cards and reports on readiness, and include these entities in cyber exercises that the Maryland Emergency Management Agency (“MEMA”) conducts with DoIT, the National Guard, and other agencies.

Senate Bill 69 views cyber events as potentially having the same catastrophic effects as floods, wildfires, or other natural events. The bill will leverage the natural convening power and existing relationships that MEMA has with other State agencies and with local units of government. The bill will also provide additional resources to MEMA to execute this new mission.

The Office also recommends this Committee consider North Dakota Senate Bill No. 2110<sup>1</sup> as a reference on how Maryland should enlarge DoIT's role with respect to the other branches of State government as well as local governments and the public university system.<sup>2</sup>

In sum, SB 69 provides an active support to prepare against cybersecurity attacks through MEMA and DoIT coordination.

cc: Committee Members

---

<sup>1</sup> See generally S.B. 2110 (N.D. Jan. 3, 2019), <https://www.legis.nd.gov/assembly/66-2019/documents/19-8091-04000.pdf>.

<sup>2</sup> See MD. CYBERSECURITY COUNS., MARYLAND CYBERSECURITY COUNCIL ACTIVITIES REPORT 2017 - 2019, 26 (July 1, 2019), <https://www.umgc.edu/documents/upload/maryland-cybersecurity-council-activities-report-2017-2019.pdf>.

**SB69LOI.pdf**

Uploaded by: Kelly, Catherine

Position: INFO





LARRY HOGAN  
GOVERNOR  
COMMANDER-IN-CHIEF

STATE OF MARYLAND  
MILITARY DEPARTMENT  
FIFTH REGIMENT ARMORY  
BALTIMORE, MARYLAND 21201-2288

TIMOTHY E. GOWEN  
MAJOR GENERAL  
THE ADJUTANT GENERAL

January 29, 2021

Senator Paul Pinsky, Chair  
Senate Education, Health and Environmental Affairs Committee  
2 East, Miller Senate Office Building  
Annapolis, Maryland 21401

RE: SB 69 – Maryland Emergency Management – Cybersecurity Coordination and Operations Office - Establishment

Dear Chairman Pinsky:

I am writing to share information regarding the above referenced Senate Bill.

Senate Bill 69 establishes the Cybersecurity Coordination and Operations Office within the Maryland Emergency Management Agency (MEMA) and requires the Director of MEMA to appoint an Executive Director as head of the Office. The proposal requires the Office to be provided with sufficient staff to perform the Office's functions and defines those functions. It also requires the Office to establish regional assistance groups to deliver or coordinate support services to political subdivisions, agencies, or regions.

The Maryland Department of the Military has many cybersecurity mission based units. Within the Air Guard, there are almost 300 Airmen within the 175th Cyber Operations Group located at both Warfield Air Base and soon at Ft. Meade, with a mix of full and part time individuals. Within this unit, they have an Active Duty mission of both cyber offense and defense supporting the United States Cyber Command. They have both an offensive and defensive unit mobilized with over 50 individuals supporting.

Within the Army Guard, their major cybersecurity unit is the 169th Cyber Protection Team with 39 full time Soldiers currently stationed at Laurel Armory and moving to the Army Research Lab in Adelphi. Finally, within the Maryland Defense Force, there is a 12 member cyber unit located at Camp Fretterd. Their mission is to support the Military Department along with the Army and Air Guard units with specific cybersecurity skill sets.

All of these units can be utilized within State Active Duty to support organizations like local governments and/or law enforcement agencies. This request for support is driven through the Governor's office through the Maryland Emergency Management Agency and the Maryland Joint Operations Center. In general, these requests would come at a time of cyber emergency (like a weather emergency when local capabilities are overwhelmed) and would be supported to defend these agencies. During non-emergency times, our members have partnered with the State Police and State Board of Elections as examples of our integration within the state. Also note, offensive capability is not legal unless operating in an Active Duty status and are therefore not able to be used within the state. The provisions of SB 69 reach far beyond current operations.

The Maryland Military Department is not able to perform the functions required in the SB 69 with existing resources. In order to create this office, the department would need to hire PIN positions to conduct the duties outlined in the Bill. The Department would need to hire 4 new staff members. The fiscal note reflects the first fiscal cycle would require over \$330,000 in FY22 to fund the resources needed to establish and operate the proposed Cybersecurity Coordination and Operations Office. The costs for the subsequent fiscal cycles grow exponentially.

Maryland has had numerous cyber-attacks in recent years. Baltimore County, Baltimore City and Dorchester County have recently suffered the consequences of cyber-attacks. These incidents impacted the ability of local communities to carry out normal government functions. In each of these cases, state resources augmented local response activities. In addition, the Federal government recently suffered significant disruption because of the SolarWinds attack that was conducted by a foreign actor.

MEMA is an expert in conducting planning, training, and exercise preparedness activities, having successfully led countless coordination efforts to prepare agencies for a myriad of threats and hazards. In addition, MEMA coordinates the statewide response to consequence management incidents, regardless of origin of the threat. MEMA is able to succeed in both of these activities because of their relationships and close coordination with local emergency managers throughout the state.

It is our hope that this information will be heavily weighted as the Committee considers SB 69.

Thank you for your support of the Maryland Military Department. We would be happy to provide additional information if required. Please feel free to reach out by e-mail [catherine.a.kelly26.nfg@mail.mil](mailto:catherine.a.kelly26.nfg@mail.mil) or by phone 410-446-5390.

Sincerely,

*Catherine A. Kelly*

Catherine Kelly  
Director, Legislative and Government Affairs