

Yelin Testimony - SB981 2024.pdf

Uploaded by: Ben Yelin

Position: FAV



FAVORABLE WITH AMENDMENTS – SB0981

SB0891 - LOCAL CYBERSECURITY PREPAREDNESS AND LOCAL CYBERSECURITY SUPPORT FUND - ALTERATIONS

EDUCATION, ENERGY AND THE ENVIRONMENT

MARCH 7, 2024

Chair Feldman, Vice Chair Kagan and Members of the Committee:

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. I also served as the co-chair, with Senator Hester, of the Ad Hoc Subcommittee of the Maryland Cybersecurity Council on State and Local Cybersecurity. We recommended in our 2021 study that every unit of local government in Maryland conduct regular cybersecurity assessments. The General Assembly required these assessments in the 2022 cybersecurity reform legislative package.

In the years since we conducted the study and since the legislation was enacted, schools have made remarkable progress with limited resources. SB0981 will further these efforts by requiring school systems, by July 1, 2025, to take important steps to improve their cyber hygiene. First, the bill would require schools to institute a multi-factor authentication (MFA) requirement for all staff. As the sponsor has noted, current assessments indicate that only a quarter of school employees, and a smaller percentage of privileged users, currently use MFA. These days, all software has MFA as a standard feature, so this requirement would not impose an additional cost burden on school districts. The bill would also require schools to implement endpoint detection and response on all school-issued devices accessed by employees and would require school systems to invest in network monitoring. For some school districts that have not already instituted these measures, the latter requirements will add a cost burden. Thankfully, SB0981 permits the Governor to include additional money in the Local Cybersecurity Report Fund to help implement these changes, and to address the most critical gap we have in school systems, which is that many of them suffer from significant staffing shortages.

The investments in this bill reflect the vision of our 2021 study and will help schools confront increasing cybersecurity threats while also mitigating the financial burden of improving network resilience. For these reasons, we respectfully request a **favorable report** on SB0981.

SB0981 Testimony.pdf

Uploaded by: James Corns

Position: FAV

I am writing in support of Senate Bill 0981. Three years ago, Baltimore County Public Schools (BCPS) suffered a major cyberattack that caused it to close for three instructional days. The impact to the system was wide scale and long lasting. Through hard work and the support of county and state resources, BCPS was able to, not only rebuild, but re-imagine its networks and digital resources. The key to BCPS's rebuild was the use of industry standard frameworks and technical expertise to implement them. Much of this support came as a response to the cyberattack and the immediate need to rebuild key infrastructure.

SB0981 seeks to establish the support for LEAs to proactively address the security needs of their infrastructure. In Maryland, LEAs vary widely in size from systems with roughly 2,000 students up to three systems that fall in the top 25 largest systems in the county. All 24 LEAs have unique needs and limited resources to address them. SB0981 requires three of the most basic security measures to protect an LEA's systems (Multi Factor Authentication, Network Monitoring, and Endpoint Protection) and builds a mechanism for those LEAs that need additional implementation support, to receive them.

The overall impact of the attack in BCPS has been felt for years and SB0981 seeks to provide support to LEAs to mitigate their risk and hopefully spare them from the need to recover. Proactive support and achievable first steps will go a long way to ensure our collective resilience in the face of ever-evolving threats.

Overall, LEAs need support to move forward with their cybersecurity initiatives. Each LEA has unique needs and SB0981 builds a reasonable starting point, prioritizing the highest value measures and supplying centralized support to achieve them.

Cybersecurity Readiness in Maryland's Education Sy

Uploaded by: Katie Fry Hester

Position: FAV

Cybersecurity Readiness in Maryland's Education System: A Brief Overview

Scope of the Problem:

- The K12 Security Information Exchange estimates that there have been more than 1,330 publicly disclosed cyberattacks since 2016.
- In the last three years, two large school systems have suffered cyberattacks, which affected almost 250,000 students and cost millions in recovery.

State Standards and Readiness Assessment:

- The Maryland DOIT has established Minimum Security Standards for state agencies, including Maryland Local Educational Agencies (LEAs).
- In 2023, a survey was conducted with the LEAs to assess their readiness and hindrances to implementation. Of the 24 LEAs, 15 responded in various sizes.

LEA Readiness Survey Results:

- Snapshot of Schools Responding
 - 46.7% of respondents were schools between 10,001 - 49,999 students
 - 33.3% of respondents represented schools with 50,000+ students
 - 20.0% of respondents were from schools with less than 10,000 students.
- How many schools have utilized basic cybersecurity protection procedures?
 - Multi-Factor Authentication
 - 53% use some level of MFA
 - 27% had enabled MFA for all employees
 - 20% do not use MFA at all
 - Endpoint Detection and Response and Network Monitoring
 - Only 27% of LEAs felt they had adequate network monitoring and endpoint detection capabilities.
- How many LEAs felt they met the DOIT minimum standard?
 - 0%
- What resources will LEAs need to meet the standards?
 - For 22 CSF/NIST Categories in the State Minimum Security Requirements, 15 LEAs pointed to **Staffing and Skill Set/Training** as the biggest hindrance

How will SB0981 address this problem?

1. It will set an achievable starting point by prioritizing the highest value measures and supplying centralized support to achieve them.
2. It will require MFA, endpoint detection, and network monitoring of all LEAs.
3. Implements additional support for LEAs under the direction of the Director of Local Cybersecurity.

Local Cyber Preparedness_Fund Testimony.docx.pdf

Uploaded by: Katie Fry Hester

Position: FAV

KATIE FRY HESTER
Legislative District 9
Howard and Montgomery Counties

Education, Energy, and
Environment 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

Testimony in Support of SB0981—Local Cybersecurity Preparedness and Local Cybersecurity Support Fund—Alterations

March 7, 2024

Chairman Feldman, Vice-Chair Kagan, and members of the Education, Energy, and Environment Committee:

Thank you for your consideration of Senate Bill 981 - Local Cybersecurity Preparedness and Local Cybersecurity Support Fund - Alterations, which ensures our local school systems have the tools and resources they need to meet minimum state cybersecurity standards.

The K12 Security Information Exchange estimates that there have been more than 1,330 publicly disclosed school cyber attacks since 2016. The risks of cybersecurity breaches cannot be overstated, as they jeopardize sensitive data, disrupt vital services, and inflict substantial financial losses. Here in Maryland, we had a cyberattack that targeted the Baltimore City Public School district in 2020, which ultimately incurred roughly \$10 million in recovery costs, and impeded access to remote learning for students.¹ This last August, Prince George’s County Public Schools experienced a cyberattack that hit its network servers, impacted about 4,500 district user accounts, and compromised data from 99,543 individuals.²

In 2022, we passed SB754 which required schools to do cybersecurity assessments. We found that schools are doing the best they can with limited resources. Thankfully, there are several high-return, low-cost investments that we can implement:

- 1) Multi-factor authentication (MFA):** Only 27% of all school employees, 20% of privileged users, and 8% of critical systems are currently using MFA, according to a district IT report provided by MSDE. MFA is typically included as a default feature in software, so mandating its use will incur no additional costs; however, the benefits of adding another layer of cyber defense are enormous.

¹ <https://abcnews.go.com/US/baltimore-schools-failed-fully-act-security-recommendations-cyber/story?id=96671802>

² <https://statescoop.com/maryland-schools-personal-data-cyberattack/>

- 2) **Increase Staffing** For 22 CSF/NIST Categories in the State Minimum Security Requirements, Local Educational Agencies (LEAs) pointed to staffing and skill set training as the biggest hindrance. The number one request to solve differences in asset management, risk assessment, risk management, data security, information protection processes, continuous monitoring, response planning and recovery – was staffing.
- 3) **Procure standard cybersecurity tools:** LEAs need to remediate priority technical solutions now that they have completed their vulnerability assessments. These include network monitoring systems and endpoint detection, as well as more unique problems.

SB0981 puts forth a proactive response to these pressing challenges by establishing a dedicated fund to bolster cybersecurity preparedness at the local level. Specifically, the bill will:

1. Increase funding in the local cyber fund, which can be used flexibly for IT improvements such as upgrading devices, procuring new systems, training, hiring, conducting assessments, etc.
2. Require school systems to do 3 things:
 - a. Establish MFA for school employees,
 - b. Implement endpoint detection, and
 - c. Implement network monitoring systems.
3. Provide sufficient human resources at the Department of Information Technology to provide shared Information Security Officers to support the schools short on staff.

By furnishing essential financial support to our local agencies, SB0981 will help to ensure that we are protecting the financial investment the state makes in our local school systems and the data of the students and employees remains as safe as possible

For these reasons, I respectfully request a favorable report on SB0981.

Sincerely,

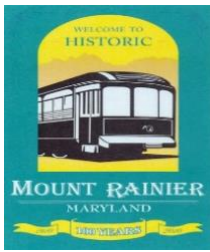


Senator Katie Fry Hester
Howard and Montgomery Counties

Favorable Support for Senate Bill 981.pdf

Uploaded by: Mayor Celina Benitez

Position: FAV



Office of The Mayor Celina R. Benitez

1 Municipal Place, Mount Rainier, Maryland 20712 Telephone: (301) 985-6585 MountRainierMD.org

Favorable Support for Senate Bill 981

Dear Honorable Chair Senator Feldman, vice Chair Senator Kagan and Members of the Education, Energy, and the Environment Committee,

I am Mayor Celina Benitez of the City of Mount Rainier, and I write to you today in strong support of Senate Bill 981, "Local Cybersecurity Preparedness and Local Cybersecurity Support Fund - Alterations." In an era where cybersecurity threats are increasingly sophisticated and pervasive, the provisions of SB 981 are not just necessary; they are critical to safeguarding the integrity of our local governments and school systems.

The bill's proposal to authorize a \$10,000,000 appropriation for the Local Cybersecurity Support Fund for fiscal years 2026 and 2027 demonstrates a proactive and strategic approach to enhancing our cybersecurity infrastructure. This funding is essential for cities like Mount Rainier, enabling us to fortify our defenses against cyber threats that jeopardize the privacy, security, and welfare of our citizens.

Additionally, SB 981's requirement for the Department of Information Technology to provide sufficient information security officers to assist the Director of Local Cybersecurity will significantly bolster our local governments' capacity to respond to and mitigate cybersecurity risks. The expertise and support of information security officers are invaluable resources in our ongoing efforts to protect our digital infrastructure.

Of particular note is the bill's mandate for local school systems to implement multifactor authentication, endpoint detection and response on all system-owned devices, and network monitoring by July 1, 2025. These measures are critical in protecting the data and privacy of our students, faculty, and staff. In the City of Mount Rainier, we believe in the paramount importance of securing our educational institutions from cyber threats, which not only pose risks to information security but also to the safety and well-being of our children.

Senate Bill 981 presents a comprehensive and forward-thinking approach to enhancing cybersecurity preparedness across Maryland. By supporting this bill, we are not only investing in the technological resilience of our local governments and school systems but also in the safety and security of our communities.

I urge the committee to favorably Support for SB 981 and to recognize the importance of robust cybersecurity measures in safeguarding the future of our state.

Please feel free to contact me at 301-985-6585 or via email MayorBenitez@MountRainierMD.org if you have any questions.

Sincerely,

Celina R. Benitez

Mayor Celina Benitez, City of Mount Rainier

RJR-(Varonis) SB981 Letter (SUPPORT)(2024).pdf

Uploaded by: Jason Bonasera

Position: FWA



Senator Brian Feldman, Chair
Senator Cheryl Kagan, Vice-Chair
Senate Education, Energy, and the Environment Committee
Miller Senate Office Building, 2 West
Annapolis, Maryland 21401

Re: *Senate Bill 981: Local Cybersecurity Preparedness & Local Cybersecurity Support Fund – Favorable w/ Amendments*

March 6, 2024

Dear Chairman Feldman and Committee Members:

On behalf of Varonis Systems, I would like to take this opportunity to thank you for the opportunity to submit this letter of support with amendments to Senate Bill 981: *Local Cybersecurity Preparedness & Local Cybersecurity Support Fund*.

As written, Senate Bill 981 would authorize the Governor (in FY26 and FY27), to include in the annual budget bill an appropriation of \$10,000,000 for the Local Cybersecurity Support Fund. The Fund was established through the enactment of Chapter 241 - *Local Cybersecurity Support Act of 2022 (Senate Bill 754)*. The purpose of the Fund is to provide financial assistance to local governments to improve cybersecurity preparedness, including but not limited to network/device upgrades; recruitment; hardware/software support; training; and cybersecurity assessments.

Major data breaches from the past few years are reminders that cybersecurity can't remain an afterthought when it comes to budgeting priorities. The threat landscape is expanding and the likelihood of a cyber-attack is high. Luckily, more companies are taking their strategy seriously since investments in [cybersecurity budgets increased by 141 percent between 2010 and 2018](#).

In an article, titled "*The Future of Cybersecurity Budgeting*", Michael Buckbee stated, "companies are increasing their cybersecurity budgets". He further said, "the key to successfully using a cybersecurity budget relies on the relationship between top leadership and cybersecurity professionals. A company's overall security posture can improve if everyone is on the same page about budget allocations and how they impact the business." The same philosophy holds true for both state and local governments.

The investments made into strategic cybersecurity efforts towards increasing efficiency and decreasing response times will pay off for companies in the long run. With the recent recorded cyber attacks (and threats) to the State's departments and school systems, it is imperative for the State of Maryland to make these laudable investments now in order to avert future incidents.

In addition, Senate Bill 981 would require the Department of Information Technology (DoIT) to provide additional information security officers to assist (and support) the Director of Local Cybersecurity.

Finally, the bill would require that, by July 1, 2025, a local school system to implement for all school employees multifactor authentication, endpoint detection and response on all system-owned devices, and network monitoring. We believe this section of the bill could be strengthened to reflect the following friendly amendments:

Amendment No.1 – Page 5, line 26: **STRIKE** the word “AND”.

Amendment No.2 – Page 5, Line 27: **INSERT** the following, “**(3) DATA MONITORING DETECTION AND RESPONSE ON ALL SYSTEM DATA REPOSITORIES; AND**”

Amendment No. 3 – Page 5, Line 27: **STRIKE** “(3)” and **INSERT** “(4)”.

It is for these reasons that Varonis supports the passage of Senate Bill 981, with the aforementioned amendments, and urges this committee to give this legislation a FAVORABLE report.

Thank you for your consideration and time.

Sincerely,



Jason Bonasera
Varonis Systems, Inc.

SB 981.Cyber Security Funding and Mandated Reforms

Uploaded by: John Woolums

Position: FWA



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

BILL: Senate Bill 981
TITLE: Local Cybersecurity Preparedness and Local Cybersecurity Support Fund - Alterations
DATE: March 7, 2024
POSITION: SUPPORT WITH AMENDMENTS
COMMITTEE: Education, Energy, and the Environment
CONTACT: John R. Woolums, Esq.

The Maryland Association of Boards of Education (MABE) supports Senate Bill 981 as it is intended to ensure major increased investments of \$10 million annually to the Local Cybersecurity Support Fund. However, MABE requests an amendment to remove the strict, deadline-based, mandate that all school systems implement multifactor authentication for all school employees and provide endpoint detection and response on all system-owned devices accessed by employees By July 1, 2025.

Several cybersecurity bills were enacted in 2022 to address state and local government policies and practices toward the goal of major overhauls and upgrades in cybersecurity, including the creation of the Local Cybersecurity Support Fund. School systems were included in these new laws, and are working to with the Department of Information Technology (DoIT) to implement the many cybersecurity assessments, reports, and enhancements called for under these recent laws.

However, MABE opposes the manner in which this bill would mandate local school system compliance with the bill's new cybersecurity standards. The bill is simply too specific and prescriptive regarding the measures school systems would be mandated to have in place by mid-2025. Therefore, MABE requests amendments to remove these provisions of the bill.

MABE, on behalf of all local boards of education, certainly appreciates and supports the need for increased investments in the security of all school system information technology systems. 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. MABE appreciates that Senate Bill 981 highlights the need for increased state spending on school system cybersecurity, but by authorizing and not mandating state funding in future budgets, the bill may fail to adequately address the costs imposed by the bill. In addition, the \$10 million identified in the bill would not be sufficient nor provided in time to assist local school systems in fulfilling all of the bill's requirements.

Local school systems support continued efforts to identify and dedicate the additional state and local resources needed to ensure continuous improvement in cybersecurity across all state agencies and among Maryland's diverse array of local governments and school systems. And MABE assures the legislature that on behalf of local school systems we are working in 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 981 with the amendments described above.

SB0981-EEE_MACo_SWA.pdf

Uploaded by: Kevin Kinnally

Position: FWA



Senate Bill 981

Local Cybersecurity Preparedness and Local Cybersecurity Support Fund - Alterations

MACo Position: **SUPPORT**
WITH AMENDMENTS

To: Energy, Education, and the Environment
and Budget and Taxation Committees

Date: March 7, 2024

From: Kevin Kinnally

The Maryland Association of Counties (MACo) **SUPPORTS SB 981 WITH AMENDMENTS**. This bill generally modifies and expands the purpose of the Local Cybersecurity Support Fund. MACo requests amendments to bolster support for local cybersecurity efforts and ensure a strategic, coordinated, and flexible approach to enhancing cybersecurity preparedness across the state.

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.

This bill authorizes the governor to include in the annual budget bill for fiscal 2026 and 2027 an appropriation of \$10 million to the Local Cybersecurity Support Fund, requires the Department of Information Technology (DoIT) to provide sufficient information security officers to assist the director of Local Cybersecurity in the execution of their duties, and mandates that local school systems implement specified cybersecurity measures.

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 delivering essential services. As such, MACo urges the General Assembly to mandate the allocation of needed resources to help lead local governments, school systems, and critical infrastructure toward a more cyber-secure future.

Further, while MACo appreciates the bill's intent to provide direct financial assistance to local governments to improve cybersecurity preparedness, some local governments could benefit from DoIT providing direct support services like shared service agreements, 24/7 network monitoring, real-time incident response, statewide risk assessments, and training. As such, MACo requests that the Fund be available for direct financial assistance and state-provided services to ensure an equitable approach to cyber preparedness and resilience across Maryland.

Accordingly, MACo urges the Committee to issue a **FAVORABLE WITH AMENDMENTS** report on SB 981.

MD K12 TLF TLFCC SB981.pdf

Uploaded by: Richard Lippert

Position: FWA



Maryland K12 Technology Leadership Forum Board

TO: Senate Education, Energy, and the Environment Committee

FROM: Maryland K12 Technology Leadership Forum

RE: Senate Bill 981 – Local Cybersecurity Preparedness and Local Cybersecurity Support Fund
- Alterations

DATE: March 5, 2024

POSITION: Support with Amendments

The Maryland K12 Technology Leadership Forum (MDK12 TLF or TLF) is an independent organization representing Information Technology (IT) personnel from all 24 Maryland Local Education Agencies (LEAs). The purpose of the TLF is to hold a collaborative forum for the support and advocacy of technology issues related to Public K12 Education in Maryland. The TLF is governed by a representative Board of the CIO's/Information Technology Leaders of all 24 LEAs in Maryland.

The MDK12 TLF Cybersecurity Committee (MDK12 TLFCC or TLFCC) is an independent committee authorized by the TLF to coordinate and share K-12 cybersecurity information, initiatives, and opportunities with each of the 24 LEAs and our partners around the state. The membership of the TLFCC is made up of the TLF and any other LEA employees that deal with school system cybersecurity.

Maryland Public Schools need personnel and resources in the fight against cybersecurity threats. Public Schools have increasingly become the number one target of cyber criminals. Maryland school systems hold personal and confidential information on more than 890,000 students, 128,000 active employees, and countless retirees from across the state. Maryland school districts have been the target of cybersecurity attacks that have interrupted our mission of education and our duty to protect the vital data entrusted to us. The proposed \$10 million is a good beginning amount but not adequate to fully fund the initiatives in the bill. If all \$10 million were to be distributed to the 24 LEAs, it would equate to approximately \$6.25 per user (students and active staff members) that must be safeguarded against cybersecurity threats. Future increases in the amount of funding and staffing are needed for all school districts.

The MDK12 TLF and TLFCC jointly support Senate Bill 981 with Amendments.

The amendments recommended by the TLF and TLFCC are:

- 1) Under § 3.5–407 (b)(2) the wording to be changed to “complete a third-party cybersecurity preparedness assessment.”
- 2) Remove § 3.5–407 (c) as this is encompassed by the new language in (b)(2).
- 3) Under § 3.5–405 include language to require a minimum of one cybersecurity training for all employees or more as deemed necessary by the local school system.
- 4) Add wording for the priority of the additional \$10 million funding.
 - a. First priority for school districts to meet requirements under § 3.5–405.
 - b. Second priority for regional information security officers.



Maryland K12 Technology Leadership Forum Board

- c. Third priority for school districts to procure and implement cybersecurity measures as outlined in the bill to increase their cybersecurity maturity.

MD SB981-2024 Amendments.pdf

Uploaded by: Vennard Wright

Position: FWA

March 6, 2024

The Honorable Katie Fry-Hester
Maryland State Senate
James Senate Office Building, Room 202
11 Bladen St., Annapolis, MD 21401

Dear Senator Fry-Hester,

I hope this letter finds you well. My name is Vennard Wright, and I am writing to you in my capacity as the former Chief Information Officer (CIO) for Prince George's County, MD, and WSSC Water. With a career dedicated to enhancing technological infrastructure and ensuring the cybersecurity of public services, I have observed firsthand the critical importance of robust cybersecurity frameworks, especially at the local level.

I am reaching out to express my support for Maryland Senate Bill 981, which aims to establish the Local Cybersecurity Preparedness and Local Cybersecurity Support Fund. This bill signifies a vital step forward in our collective effort to safeguard Maryland's digital infrastructure from evolving threats. However, I would like to propose specific amendments to enhance its effectiveness based on my professional experience.

The proposed legislation mandates the Department of Information Technology (DoIT) to interact primarily with Emergency Managers for the implementation and coordination of cybersecurity measures. While Emergency Managers play an integral role in our state's safety and preparedness strategies, they are typically not cybersecurity subject matter experts (SMEs). This could inadvertently create a bottleneck and add an unnecessary layer of communication during critical times, such as a data breach or cyber-attack.

To address this concern, I propose the following amendment to the bill:

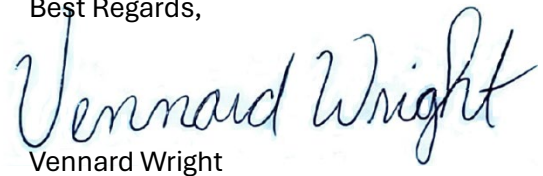
Amendment Proposal: Require the Department of Information Technology (DoIT) to establish direct communication channels with local IT officials, including CIOs and IT Managers, in addition to Emergency Managers. This approach will facilitate real-time sharing of information and swift implementation of mitigation strategies during cybersecurity incidents. Local IT officials are equipped with the specific technical expertise required to address cybersecurity threats effectively and should be integral to the communication loop.

This amendment does not undermine the importance of Emergency Managers but rather enhances the overall response capability by leveraging the specialized skills of local IT professionals. By ensuring that local IT officials are directly involved, we can improve the responsiveness and efficiency of our cybersecurity initiatives.

I believe that with these amendments, Maryland Senate Bill 981 will offer a more comprehensive and practical framework for bolstering our local cybersecurity infrastructure. I am available to discuss this proposal in more detail and provide further insights based on my experience in the field.

Thank you for your consideration of these amendments and for your ongoing commitment to the cybersecurity and welfare of Maryland's communities. I look forward to the possibility of working together to strengthen our state's defenses against cyber threats.

Best Regards,

A handwritten signature in blue ink that reads "Vennard Wright". The signature is written in a cursive style with a large initial "V".

Vennard Wright