SB0825_–_Public_Safety_–_Critical_Infrastructure_P
Uploaded by: Cecilia Plante
Position: FAV

TESTIMONY
SB0825 – Public Safety – Critical Infrastructure Protection

Bill Sponsors: Senator Hester
Committee: Education, Energy, and the Environment
Organization Submitting: Maryland Legislative Coalition
Person Submitting: Aileen Alex, Co-Chair
Position: FAVORABLE

I am submitting this testimony in support of SB0825 on behalf of the Maryland Legislative Coalition. We are an association of unpaid citizen advocates—individuals and grassroots groups in every district across the state—representing and supporting more than 30,000 Marylanders.

At a time when federal efforts to protect critical infrastructure are inconsistent and subject to shifting priorities, Maryland cannot afford to just hope for national action. The measures contained in SB0825 help safeguard the systems Marylanders rely on every day— water and wastewater systems, transportation networks, telecommunications infrastructure, hospitals, emergency response facilities, and other essential public safety and communications systems.

SB0825 establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center and directs the Maryland Department of Emergency Management to take defined actions whenever these systems are threatened or attacked.

The bill also requires the Department of Information Technology to provide clear cybersecurity reporting standards and Information Sharing and Analysis Center-type access for infrastructure owners and operators, strengthening statewide coordination, information sharing, and readiness against both physical and cyber threats.

This legislation aligns with the mission of the Maryland Legislative Coalition. Our work centers on transparency, accountability, and preventing harm. Strengthening critical-infrastructure protection directly supports those values by ensuring Marylanders can trust that the systems they depend on are secure and resilient.

For these reasons, we respectfully urge a **FAVORABLE** report on SB0825.

Written Testimoy for SB825_HB1239-Cleary.pdf
Uploaded by: Chris Cleary
Position: FAV

Chair, Vice Chair, and Members of the Committee:

Thank you for the opportunity to submit written testimony in strong support of SB825/HB1239, which establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center (MCAC).

I previously served as the Principal Cyber Advisor for the Department of the Navy. In that role, I advised senior civilian and uniformed leadership on cyber risk, operational readiness, and the security of the systems that enable naval and Marine Corps missions worldwide. One of my leading efforts during that time was elevating awareness of a structural vulnerability that often receives insufficient attention: much of the infrastructure that enables Department of Defense mission execution is not owned or operated by the federal government. It is owned and operated by state and local governments and private industry.

Installations depend on local power grids. Shipyards depend on municipal water systems. Communications infrastructure that supports operational command and control frequently traverses commercial networks. Transportation hubs that move personnel and materiel are state-managed assets. In short, the ability of the Department of the Navy—and the broader Department of Defense—to project power depends in significant part on infrastructure that sits outside federal control. From that vantage point, it became clear to me that critical infrastructure protection is not just a federal issue. It is a state responsibility with direct national security implications. SB825/HB1239 reflects precisely that understanding.

Threats to critical infrastructure are no longer speculative. They are persistent, sophisticated, and increasingly integrated across cyber and physical domains. In recent years, activity targeting U.S. infrastructure has not only increased, but public acknowledgment of that activity by senior national security leaders has increased as well. In a recent interview on 60 Minutes, the former Commander of United States Cyber Command and Director of National Security Agency publicly discussed adversary “pre-positioning” inside U.S. critical infrastructure. He acknowledged that the People’s Republic of China has established access within portions of U.S. infrastructure—not to cause immediate disruption, but to hold those systems at risk during a potential crisis or conflict.

That is what “pre-positioning” means: gaining and maintaining access in advance, creating the ability to impose consequences at a time of their choosing. When leaders at that level speak openly about adversary presence inside infrastructure, it signals something important. This is no longer an abstract warning from analysts. It is an operational reality being addressed at the highest levels of government.

We have seen Chinese cyber actors probe energy and water systems. We have seen ransomware operations disrupt hospitals and municipal services. We have seen information operations target public confidence in essential services. These activities are not random. They are deliberate shaping operations designed to create leverage, impose costs, and constrain decision-making during a crisis. Maryland hosts military installations, federal facilities, transportation hubs, biotechnology assets, and defense contractors that would be strategically relevant in any national emergency. Pre-positioning inside infrastructure in this state would have consequences well

beyond Maryland's borders. The resilience of Maryland's infrastructure is therefore not only a matter of state governance—it is directly tied to national defense readiness. The lesson is clear: we do not get a warning shot.

Critical infrastructure is not a collection of isolated assets. It is a networked system of systems. Power supports water. Water supports hospitals. Communications support emergency services. Transportation supports supply chains. An attack on one node can cascade across sectors in ways that are difficult to predict in the moment. That reality demands organized, deliberate analysis in advance of crisis. SB825/HB1239 recognizes this by directing the state to analyze threats holistically, prioritize assets based on cascading impact, map interdependencies, develop coordinated response plans, and engage directly with critical infrastructure sector leaders. This is not duplication of existing efforts. It is integration of them.

Maryland is uniquely positioned. We host major federal facilities, defense contractors, biotechnology firms, transportation hubs, and energy infrastructure. The state's economic and national security footprint is significant. The Maryland Coordination and Analysis Center already plays a critical role in information sharing. Establishing a dedicated Critical Infrastructure Protection Branch within MCAC centralizes analytic capability focused specifically on infrastructure risk, strengthens public-private coordination before a crisis occurs, and enables prioritization based on impact rather than anecdote. In the cyber domain, speed and integration win. Organizational clarity is a prerequisite to both.

Adversaries move continuously. Bureaucracies move episodically. The question before this committee is not whether Maryland faces infrastructure risk. It does. The question is whether the state organizes proactively or waits for a catalyzing event to force reorganization under pressure. History consistently shows that it is far more expensive—financially, socially, and operationally—to rebuild resilience after a disruption than to establish coordination before one.

From my experience at the Department of the Navy, I can say with confidence that state-level infrastructure resilience is inseparable from national defense readiness. Maryland does not need to reinvent the wheel. It needs to align the spokes. SB825/HB1239 provides a mechanism to integrate analysis, prioritize risk, coordinate with industry, and prepare for cascading impacts in a disciplined and sustainable way.

The threats to critical infrastructure are real, present, and accelerating. The cost of inaction will not be measured only in dollars, but in public confidence, economic stability, and operational continuity. The question is not whether we can afford to prepare — it is whether we can afford not to. Adversaries are already organized. Maryland should be too.

Respectfully submitted,
Chris Cleary

Senate Bill 825_thetac_fav.pdf
Uploaded by: Chris Hollifield
Position: FAV

Technology Advancement Center

Senate Bill 825 – Public Safety – Critical Infrastructure Protection

Position: Support

The Technology Advancement Center (TAC) is a non-profit whose mission is to create and propel enduring technological advantages for our state and nation. Through collaboration with small business, academic researchers and non-traditional members, TAC serves as an intermediary and helps Maryland businesses and communities stay secure and innovative.

Maryland's critical infrastructure—energy, transportation, healthcare, and more—is the backbone of our daily lives. SB 825 creates a **Critical Infrastructure Protection Branch** to make sure these systems are **watched, prioritized, and protected** before anything goes wrong.

SB 825 achieves this, in part, by focusing on **collaboration**. By connecting private infrastructure owners with state cybersecurity guidance and information sharing, Maryland ensures that **both government and business are working together**, not in silos. The only way Maryland and our nation can combat threats and prevent emergencies is to make sure private and public entities are supporting each other.

In short, SB 825 makes Maryland smarter, safer, and ready for the challenges of today and tomorrow. TAC urges a favorable report for SB 825.

For more information contact thetac.tech

7000 Columbia Gateway, Suite 150, Columbia, MD 21046 **443-626-4450**

MML- FAV- SB 825.pdf
Uploaded by: Iris Ibegbulem
Position: FAV

TESTIMONY

COMMITTEE:	Senate Education, Energy, and the Environment	**DATE:**	March 5, 2026
POSITION:	Favorable	**BILL:**	SB 825

The Maryland Municipal League (MML) supports Senate Bill 825, Public Safety - Critical Infrastructure Protection. Municipalities and local governments own, operate, or directly support a portion of the State's critical infrastructure including water and wastewater systems, local public safety communication networks, and transportation corridors. These systems are essential to the daily safety and economic stability of countless communities in the State. SB 825 provides a clear framework to strengthen coordination, threat assessment, and response planning across these assets.

SB 825 creates a statewide structure with well-defined leadership and direct accountability for coordinating critical infrastructure security efforts, allowing municipalities, infrastructure owners, and local stakeholders to have meaningful, structural support. By allowing local critical infrastructure owners statewide to engage with the Maryland Information Sharing and Analysis Center, the bill increases coordinated information exchange, increases local awareness of emerging threats, and supports standardized reporting practices.

The State of Maryland has been hit by bad actors before with a memorable ransomware attack on the Maryland Department of Transportation in 2025. Anne Arundel County had a cyber incident in 2025 as well which affected their government operations and network while Baltimore City's ransomware attack in 2019 affected the city's most critical systems. Municipalities and local governments face an elevated risk of disruption to critical systems and infrastructure due to limited resources and by establishing a singular point of accountability, local governments will benefit immensely. Senate Bill 825 advances public safety by aligning government and infrastructure partners to protect the essential systems that Maryland residents depend on without interruption.

For these reasons, the League respectfully requests that the committee provide Senate Bill 825 with a favorable report.

For more information relating to this piece of testimony, please contact:

Iris Ibegbulem: Manager, Advocacy and Public Policy, irisi@mdmunicipal.org

SB825 Testimony.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

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

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

Testimony in Support of SB 825 - Public Safety - Critical Infrastructure Protection

March 3, 2026

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

Thank you for your consideration of Senate Bill 825, which establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center (MCAC) and creates clear, statewide measures to protect Maryland's critical infrastructure from cyber and physical threats.

Recent unclassified threat briefings make clear that modern adversaries increasingly seek to disrupt essential systems rather than rely on traditional physical attacks. Energy, water, transportation, communications, and food systems are now primary targets because disruption can create widespread economic and social instability without a single kinetic strike. Lessons from cyber operations observed in Ukraine and rising geopolitical tensions in the Indo-Pacific demonstrate that these threats are no longer hypothetical. Nation-state actors are actively probing U.S. infrastructure networks through persistent low-level intrusions designed to test vulnerabilities and maintain access.

As the traditional separation between information technology and operational technology disappears, physical infrastructure is increasingly exposed to foreign cyber intrusion. Recent examples include:

- Water & Energy — The FBI, NSA, and CISA have warned that Volt Typhoon, a state-sponsored Chinese hacker group, has already compromised the IT environments of multiple energy and water organizations as part of an effort to pre-position themselves on critical IT networks in the case of future crisis or conflict with the United States.[1]
- Transportation — In 2025, the Rhysida ransomware group claimed responsibility for breaching the Maryland Transit Administration's network and demanded $3.4 million,

[1] https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

causing system outages that affected customer-facing platforms and internal operations and requiring the agency to shift to manual processes during recovery.[2]

- Telecommunications — In late 2024, the state-sponsored Chinese hacker group Salt Typhoon infiltrated multiple U.S. telecommunication companies, including internet service providers.[3] Federal authorities report that this may have been an effort to gain access to communications between then-presidential candidates Kamala Harris, J.D. Vance, and Donald Trump.[4]
- Healthcare — Iranian government-sponsored cyber actors targeted Boston Children's Hospital in a "despicable" attempt to disrupt patient care, as characterized by FBI Director Christopher Wray.[5]

Last year, this Committee strengthened cybersecurity protections for Maryland's water systems through Senate Bill 871. However, protecting individual sectors alone is no longer sufficient. Maryland must adopt a comprehensive, statewide strategy that recognizes the interdependence of critical infrastructure systems.

During the interim, I participated in Colorado's Interlock Critical Infrastructure Briefing, where state leaders described how fragmented oversight limited preparedness. Colorado responded by creating a whole-of-state partnership uniting federal agencies, state government, the National Guard, law enforcement, and private-sector operators. Their model maintains a centralized infrastructure database, conducts regular cross-sector exercises, and validates contingency plans through ongoing coordination. They have also mapped infrastructure interdependencies, recognizing that disruption in one system—such as electric power—can cascade into failures across water treatment, healthcare delivery, communications, and transportation networks.

After returning to Maryland, I found that while many agencies are doing strong work within their missions, the State lacks a comprehensive framework integrating federal, state, and local partners. Maryland needs the ability to assess cyber threats alongside potential physical impacts, understand cross-sector dependencies, and coordinate planning and response before a crisis occurs.

SB 825 addresses this gap. Developed in collaboration with the Department of Homeland Security, the Maryland Department of Emergency Management, and the National Guard, the bill establishes a Critical Infrastructure Protection Branch within MCAC to coordinate agencies responsible for overseeing critical infrastructure statewide.

---

2 https://industrialcyber.co/transport/rhysida-ransomware-gang-claims-maryland-transit-administration-breach-demands-3-4-million/

3 https://www.congress.gov/crs-product/IF12798

4 https://www.cbsnews.com/news/trump-vance-potential-targets-china-backed-hacking-operation/

5 https://www.cbsnews.com/boston/news/boston-childrens-hospital-cyberattack-iran-indictments/

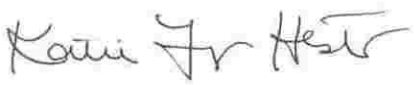
The Branch is charged with:

1. Analyzing potential threats and prioritizing critical infrastructure assets, including understanding vulnerabilities that could arise in the event of an attack;
2. Strengthening critical infrastructure assets within the State that are identified as priorities;
3. Working with the Maryland Department of Emergency Management (MDEM) to map cascading impacts of an attack on critical infrastructure and create response plans;
4. Working with the Department of Information Technology (DoIT) to provide up-to-date cybersecurity reporting standards to owners and operators of critical infrastructure;
5. Collaborating with MDEM to respond to attacks if they happen;
6. Coordinating with the Governor's Office of Homeland Security and critical industry, local, and federal counterparts on issues pertaining to critical infrastructure.

SB825 ensures Maryland is prepared to confront evolving threats. Our critical infrastructure provides essential services including healthcare, communications, and water access. Maryland residents and agencies have already experienced the consequences of cyber disruptions. This legislation positions the State to be proactive rather than reactive.

For these reasons, I respectfully request a favorable report on SB825.

Sincerely,



Senator Katie Fry Hester
Howard and Montgomery Counties

SB0825-EEE_MACo_SUP.pdf
Uploaded by: Kevin Kinnally
Position: FAV

MARYLAND Association of COUNTIES

Senate Bill 825

Public Safety - Critical Infrastructure Protection

MACo Position: **SUPPORT**

To: Education, Energy, and the Environment Committee

Date: March 5, 2026

From: Kevin Kinnally

The Maryland Association of Counties (MACo) **SUPPORTS** SB 825 as a sensible step to bolster Maryland's coordination and readiness against threats to critical infrastructure.

This bill establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center to strengthen threat identification, coordination, and response related to critical infrastructure. The bill formalizes a statewide structure to prioritize assets, assess vulnerabilities, coordinate across sectors, and improve information sharing on both cyber and physical threats.

Counties operate and maintain a significant share of Maryland's critical infrastructure. Local governments oversee water and wastewater systems, emergency communications, transportation assets, public buildings, IT networks, and public safety systems. Disruption to any of these systems has immediate and cascading impacts on residents and regional stability.

The bill improves coordination among state, local, federal, and private-sector partners and strengthens Maryland's ability to detect and respond to emerging threats. Furthermore, the bill appropriately situates this work within the Maryland Coordination and Analysis Center while directing collaboration with the Department of Emergency Management and the Department of Information Technology. A more integrated approach enhances preparedness and consequence management before and after an incident.

As threats grow more complex — particularly in cybersecurity and operational technology environments — Maryland benefits from a centralized structure that prioritizes risk assessment, vulnerability identification, and cross-sector communication.

For these reasons, MACo respectfully requests a **FAVORABLE** report on SB 825.

Senator Hester SB825 Support Letter.pdf
Uploaded by: Michael Centrella
Position: FAV

SecurityScorecard

The Honorable Brian Feldman
Education, Energy, and the Environment Committee
2 West, Miller Senate Office Building
Annapolis, MD 21401

Senate Bill 825 – Critical Infrastructure Protection – Support

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

I am writing to express my strong support for Senate Bill 825, which establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center.

My name is Michael Centrella. I served 25 years with the United States Secret Service, most recently as Assistant Director of Field Operations, where I oversaw investigative and protective operations nationwide. During my career, I led complex investigations involving cyber-enabled financial crimes, transnational criminal organizations, and threats impacting critical systems and public safety. Today, I work in the cybersecurity sector focused on strengthening public-sector and critical infrastructure resilience.

The threat environment facing Maryland's critical infrastructure is real and accelerating. Healthcare systems, transportation networks, schools, utilities, and local governments are increasingly targeted by sophisticated criminal organizations and foreign adversaries. These attacks are not simply technology disruptions—they are public safety events. They can delay emergency services, disrupt medical care, halt government operations, and undermine public confidence.

One of the most significant challenges states faces is fragmentation. Political subdivisions and infrastructure operators often operate independently, with varying levels of cybersecurity maturity and limited visibility into interconnected risks. Adversaries exploit these seams. A single compromised vendor or under-resourced local entity can become the gateway to broader, cascading disruption.

Senate Bill 825 addresses this challenge directly. By establishing a dedicated Critical Infrastructure Protection Branch, the State strengthens governance, centralizes coordination, and creates accountability for identifying and prioritizing risks across sectors. This structure is essential to move from reactive response to proactive protection.

Modern cyber risk extends beyond agency networks into supply chains, cloud environments, and operational technology systems. A coordinated, statewide approach to vulnerability identification and

SecurityScorecard, Inc.
1140 Avenue of Americas, 19th Floor
New York, NY 10036

Michael.Centrella@securityscorecard.io
info@securityscorecard.com
Main (800) 682-1707

threat prioritization will allow Maryland to allocate resources strategically and reduce systemic exposure before incidents occur.

Senate Bill 825 positions Maryland to lead with foresight rather than respond in crisis. For these reasons, I respectfully urge the Committee to support this important legislation.

Thank you for your consideration.

Respectfully submitted,

Michael R. Centrella

Head of Public Policy, SecurityScorecard

For any questions or more information regarding SSC's position, please contact Michael.Walsh@capitol-strategies.com

Testimony in support of SB0825 - Public Safety - C
Uploaded by: Richard KAP Kaplowitz
Position: FAV

SB0825_RichardKaplowitz_FAV
03/05/2026
Richard Keith Kaplowitz
Frederick, MD 21703-7134

TESTIMONY ON SB#0825 - POSITION: FAVORABLE
Public Safety - Critical Infrastructure Protection

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

FROM: Richard Keith Kaplowitz

My name is Richard Kaplowitz. I am a resident of District 3, Frederick County. I am submitting this testimony in support of SB#0825, **Public Safety - Critical Infrastructure Protection**

The National Governors Association, whose vice chair is Governor Moore of Maryland, has discussed the *States' Role in Addressing Foreign Threats in U.S. Critical Energy Infrastructure Sectors* [1]

> The safety and economic security of the United States are dependent on the integrity of the nation's critical energy infrastructure systems, including power, natural gas, and petroleum. Failure of critical assets in any of these systems could have catastrophic impacts on communities, businesses and national defense. Energy is also the backbone of all other critical infrastructure systems, meaning that an energy supply failure could have cascading effects on transportation, water, telecommunications, finance, healthcare and other sectors.
>
> To deter, detect, and defend these entities requires the cooperation of state government along with federal interagency partners and energy sector entities. Governors are uniquely positioned to convene these stakeholders and implement policies that address these threats.

This bill makes Maryland take affirmative steps to implement critical infrastructure in the state.

This bill will establish the Critical Infrastructure Protection Branch in the Maryland Coordination and Analysis Center; requiring the Department of Emergency Management, in consultation with the Center, to take certain action in response to an attack on the State's critical infrastructure; and requiring the Department of Information Technology to allow the owner or operator of critical infrastructure to become a member of the Maryland Information Sharing and Analysis Center and provide cybersecurity reporting standards to the owner or operator.

I respectfully urge this committee to return a favorable report on SB0825.

[1] https://www.nga.org/publications/states-role-in-addressing-foreign-threats-in-u-s-critical-energy-infrastructure-sectors/#:~:text=Reliable%20energy%20supply%20for%20public,expedited%20emergency%20support%20and%20restoration.

Senate Bill 825 - DoIT Written Testimony.docx.pdf
Uploaded by: Sara Elalamy
Position: FWA

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Education, Energy, and the Environment Committee
FROM: Department of Information Technology
RE: Senate Bill 825 - Public Safety - Critical Infrastructure Protection
DATE: March 5, 2026
POSITION: Support with Amendments

The Honorable Brian J. Feldman, Chair
Senate Education, Energy, and the Environment Committee
2 West, Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairman Feldman,

The Department of Information Technology (DoIT) respectfully submits this letter in support of Senate Bill 825, with amendments.

The Department of Information Technology (DoIT) supports the intent of this legislation to strengthen Maryland's ability to identify, assess, and protect critical infrastructure across both public and private sectors. Enhancing coordination and preparedness for cyber and physical threats is essential to maintaining continuity of government services, protecting public safety, and ensuring the resilience of Maryland's economy.

The establishment of a Critical Infrastructure Protection function within the Maryland Coordination and Analysis Center represents an important step toward improving statewide situational awareness and fostering stronger collaboration between State agencies, federal partners, and private sector infrastructure owners and operators.

At the same time, DoIT respectfully recommends several amendments to ensure that implementation of this legislation builds upon, rather than duplicates, existing State cybersecurity and risk management structures.

Recommended Amendments

1. Clarify Cybersecurity Leadership

To align with Maryland's existing governance framework, DoIT recommends clarifying that DoIT, through the Office of Security Management, maintains responsibility for statewide cybersecurity standards and oversight.

Suggested Amendment:

Clarify that DoIT directs cybersecurity efforts for units of state government critical infrastructure in coordination with the Critical Infrastructure Protection Branch, ensuring consistency with existing statewide IT security policy and risk management practices.

2. Formalize Coordination with Existing State Cyber Functions

DoIT recommends explicitly recognizing coordination with:

- The Office of Security Management
- Maryland Information Sharing and Analysis Center (MD-ISAC)

Suggested Amendment:

Require coordination with existing State cybersecurity governance structures when conducting assessments, issuing guidance, or developing response frameworks.

3. Maintain Voluntary Engagement Model

DoIT supports the bill's voluntary approach to engagement with private infrastructure owners and recommends preserving that structure.

Suggested Amendment:

Clarify that participation in assessments, reporting, and information-sharing mechanisms remains voluntary unless otherwise required under existing State or federal law.

4. Emphasize Use of Existing Information Sharing Mechanisms

To maximize efficiency and reduce administrative burden:

Suggested Amendment:

Prioritize the use of MD-ISAC as the primary mechanism for operational technology threat intelligence exchange and shared learning.

5. Align Response Authorities

To ensure clear operational roles during incidents:

Suggested Amendment:

Clarify that MDEM retains responsibility for consequence management while DoIT retains responsibility for cyber incident coordination affecting State systems and networks.

Senate Bill 825 presents an important opportunity to strengthen Maryland's critical infrastructure resilience through improved coordination, shared situational awareness, and proactive risk mitigation.

With the amendments outlined above, the legislation can enhance statewide preparedness while ensuring alignment with existing cybersecurity governance and avoiding unnecessary duplication of effort.

DoIT looks forward to continuing to work with the Committee and the bill sponsor to support the successful implementation of this initiative.

Best,

Katie Savage
Secretary
Department of Information Technology

SB 825 Information PSC.pdf
Uploaded by: Barve Barve
Position: INFO

STATE OF MARYLAND

PUBLIC SERVICE COMMISSION

Chair Brian Feldman
Education, Energy and the Environment Committee
2 West Miller Office Building
Annapolis, MD 21401

RE: **SB 825 - Information - Public Safety - Critical Infrastructure Protection**

Dear Chair Feldman and Committee Members:

The Public Service Commission (the "Commission") appreciates the opportunity to provide this informational testimony for SB 825. This bill creates a new continuous mandate that the Commission Office of Cybersecurity determine threat levels to the State's critical infrastructure in coordination with the new Critical Infrastructure Protection Branch ("Branch"). This is an active endeavor that will likely require the routine, potentially daily or weekly, dissemination of intelligence and the sanitization of classified utility data for inter-agency application. Below, the Commission identifies potential impediments to effective implementation of this bill and solutions the Committee can consider.

The Commission has identified three areas where the requirements of SB 825 may conflict with or complicate existing mandates under the Critical infrastructure Cybersecurity Act of 2023. These are as follows:

1. Proposed § 14-1403(b)(5) directs the Branch to engage critical infrastructure providers on "voluntary cyber and physical assessments." Under current Public Utilities Article (PUA) § 5-306(c)(4), regulated utilities are legally required to engage a third party for mandatory assessments every two years. Furthermore, under PUA §2-108(d)(3)(v), the Commission is mandated to support public service companies with remediating vulnerabilities. This may create a "regulatory collision." A utility might undergo a voluntary assessment with the Branch that uses different standards than the mandatory Commission assessment, which could result in contradictory findings leading to legal challenges. To avoid this issue and prevent duplicative or contradictory findings, the bill could be amended to clarify that for regulated public service companies, the Commission remains the primary authority for assessments.

2. Proposed § 14-1404(c)(2) mandates that the Department of Information Technology (DoIT) provide up-to-date cybersecurity reporting standards to owners of critical infrastructure. This appears to conflict with PUA § 5-306(d)(2), which explicitly states that the State Chief Information Security Officer must establish these processes "in

consultation with the Commission." If DoIT issues new reporting standards to utilities under SB 825 without the Commission's consultation, they may conflict with the incident reporting criteria already established and enforced through COMAR. In order to preserve its statutory role and avoid conflict, the Commission requests that § 14-1404(c) include the phrase "in consultation with the Public Service Commission" regarding utilities.

3. Proposed § 14-1404(a)(2)(vi)(4) empowers the Branch to implement operational technology architecture monitoring. The Public Service Commission holds sensitive vulnerability data protected by strict confidentiality under COMAR 20.06.02.06. Sharing "architecture monitoring" data with a non-regulatory branch in the Maryland Coordination and Analysis Center (MCAC) requires a secure, legally vetted framework that does not currently exist, so this could violate existing regulations. This could be resolved if the bill specifically designates the Branch as an authorized recipient, subject to the same confidentiality constraints, or the Commission grants necessary authorization under COMAR 20.06.02.06.

The Commission also notes generally that its role involves oversight of infrastructure owned by utilities and coordination of the information related to that infrastructure. If the Commission detects a critical vulnerability, it would be the responsibility of the utility to resolve the vulnerability and report back to the Commission in a timely manner. The bill does not specify what enforcement options are available to compel compliance. Doing so would allow the Commission to ensure successful outcomes related to the directives of this legislation.

Please contact Niki Wiggins, Director of Legislative Affairs, at irene.wiggins3@maryland.gov if you have any questions related to this informational testimony.

Sincerely,

Kumar P. Barve
Chair, Maryland Public Service Commission