

**HB 1062\_Delegate Harrison\_FAV.pdf**

Uploaded by: Delegate Andrea Harrison

Position: FAV

ANDREA FLETCHER HARRISON  
*Legislative District 24*  
Prince George's County

Economic Matters Committee

*Subcommittees*

Alcoholic Beverages

Banking, Consumer Protection,  
and Commercial Law

Worker's Compensation



The Maryland House of Delegates  
6 Bladen Street, Room 207  
Annapolis, Maryland 21401  
301-858-3919 · 410-841-3919  
800-492-7122 Ext. 3919  
AndreaFletcher.Harrison@house.state.md.us

THE MARYLAND HOUSE OF DELEGATES  
ANNAPOLIS, MARYLAND 21401

Written Testimony – HB 1062 – Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments

February 26, 2025

Good afternoon, Chair Korman, Vice-Chair Boyce, members of the Environment and Transportation Committee and members of the Health and Government Operations Committee.

I am Delegate Andrea Harrison and I'm here to present HB 1062 – Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments.

Water infrastructure is a cornerstone of Maryland's critical infrastructure, supporting millions of residents and businesses. Cyberattacks on these systems could:

- Contaminate drinking water, endangering public health.
- Disrupt services, causing widespread economic losses.
- Undermine public confidence in utilities.
- Jeopardize compliance with federal and state safety regulations.

A 2023 EPA assessment found 9% of U.S. public water systems were “critically” or “highly” vulnerable to cyberattacks. Breaches could cost \$43.5 billion in sales and \$22.5 billion in GDP losses. Alarmingly, 70% of inspected utilities violated federal cybersecurity standards. In 2023, one-third of water utilities reported a cyber breach—a 21% increase from 2021.

Recognizing this risk, Dr. Matthew Mitroka, NSA fellow with the Maryland Cybersecurity Council, conducted an in-depth analysis of Maryland's water systems. His report highlighted the urgent need for regulation/oversight, resources, and training. SB0871 implements key recommendations from Dr. Mitroka's report, aimed at enhancing resilience and safeguarding public safety:

- Governance & Policy – Designate MDE as the State Sector Risk Management Agency, mandate 24-hour incident reporting, and require cybersecurity contacts at facilities.
- Foundational Cyber Security – Ensure adoption of best practices, including Zero Trust strategies and OT security measures.

- Risk Management & Resilience – Mandate proactive risk assessments, continuity planning, and awareness of third-party cyber risks.
- Resource Management – Leverage DoITs Local Cyber resources to enhance cybersecurity support. Raise awareness of free cybersecurity tools and connect utilities to funding.
- Education & Awareness – Strengthen cybersecurity training for operators, with university and trade organization partnerships for workforce development.

Along with Dr. Mitroka's report, this bill also aligns with the MDE's Cybersecurity Action Plan for Water and Wastewater Systems, which requires legislation for implementation. It defines covered entities as those serving over 3,300 people or utilizing Information or Operational Technology as a part of their operations, which is reflected in this bill.

HB 1062 takes a proactive approach by:

- Strengthening cybersecurity oversight by designating MDE as the lead regulatory agency and requiring coordination with DoIT and MDEM to establish standards and best practices.
- Mandating cybersecurity incident reporting to the State Security Operations Center (SOC) in DoIT for community water and sewerage systems.
- Requiring risk assessments and cybersecurity plans for water systems, ensuring proactive measures against cyber threats.
- Protecting critical infrastructure security records from public access to prevent exposure of vulnerabilities

In summary, Maryland cannot wait for a catastrophic cyberattack to act. This bill establishes clear, actionable measures to protect our water infrastructure. It will ensure that 96.5% of our constituents on large water systems (such as Washington Suburban Sanitary Commission Water, City of Baltimore, City of Hagerstown, City of Frostburg as well as those on medium systems (such as the town of Mount Airy or Town of Centreville) have the necessary safeguards to protect their water.

The Maryland Cybersecurity Council Subcommittee on Critical Infrastructure unanimously supports Dr. Mitroka's report, with input from cybersecurity experts, including Howard Barr, John Abeles, Greg Von Lehmen, and Hannibal Kemerer. We also have the support from the US Department of Defense, and you will hear from John Garstka, the Director for Cyber Warfare within the Office of the Deputy Assistant Secretary of Defense for Platform and Weapon Portfolio Management, Office of the Under Secretary of Defense for Acquisition and Sustainment.

For such an indispensable resource as water, we cannot stand idle until a cyberattack targets Maryland's water supply. For these reasons, I respectfully request a favorable report on HB 1062.

# **Water Cyber Final February 702025.pptx.pdf**

Uploaded by: Delegate Andrea Harrison

Position: FAV

**SB0871- Department  
of the Environment -  
Community Water  
and Sewerage  
Systems -  
Cybersecurity  
Planning and  
Assessments**

*Senator Katie Fry Hester*



# Recent Water Cyberattacks

**EPA Memo:** 9% of public drinking water systems scanned had “critical” or “high” priority cybersecurity vulnerabilities.

**Economic Impact:** A 2020 U.S. Water Alliance report estimated that a nationwide water system disruption could result in **\$43.5 billion** in lost sales and **\$22.5 billion** in GDP damage.

**Regulatory Failures:** According to the EPA, **70% of inspected utilities** recently violated federal standards designed to prevent cyber breaches.

**Rising Threats:** **33% of surveyed water utilities** reported at least one cyber incident in 2023, up from **21% in 2021**.

## Recent Cyberattacks:

- **American Water Cyberattack** – November 2024
- **Arkansas City Water Plant Attack** – October 2024

## Russian hacking group claims responsibility for cyberattack on Indiana wastewater plant

A video from the "People's Cyber Army of Russia" claims responsibility for last week's cyberattack on the Tipton West Wastewater Treatment Plant in Indiana.

## 'Critical' cyber vulnerabilities found in many water utilities, warns EPA inspector general

The Environmental Protection Agency's Office of Inspector General said a recent assessment uncovered an urgent need for cyber remediation.

## Fears of Weakness in Water Cybersecurity Grow After Kansas Attack

White House plans a new push to boost cybersecurity in water sector after an aborted attempt last year

CYBER REPORT

## America's largest water utility hit by cyberattack at time of rising threats against U.S. infrastructure

PUBLISHED TUE, OCT 8 2024•12:28 PM EDT | UPDATED TUE, OCT 8 2024•4:14 PM EDT

# Recommendations

01	<b>Governance &amp; Policy</b>	<ul style="list-style-type: none"><li>• Officially designate MDE as State Sector Risk Management Agency.</li><li>• Supplement the Modernize Maryland Act of 2022 with a follow-on Act.</li><li>• Update Reporting Requirements, reporting incidents within 24 hours.</li><li>• WWS facilities appoint a primary point of contact for cybersecurity.</li><li>• Cyber Adoption May Require Regulation.</li></ul>
02	<b>Foundational Cybersecurity</b>	<ul style="list-style-type: none"><li>• Ensure cyber hygiene and best practices are adopted by the WWS sector.</li><li>• Adopt cybersecurity frameworks.</li><li>• OT cybersecurity</li><li>• Entities should adopt a Zero Trust strategy, tailored to fit their operation.</li></ul>
03	<b>Risk Management &amp; Resilience</b>	<ul style="list-style-type: none"><li>• Encourage organizations to understand their risk; ensure continuity of operations</li><li>• Host regular tabletop exercises.</li><li>• Awareness of 3<sup>rd</sup> party risks.</li><li>• Cybersecurity is not only digital, ensure physical security as well.</li></ul>
04	<b>Resource Management</b>	<ul style="list-style-type: none"><li>• Leverage DoIT Local Cyber</li><li>• Highlight value of prevention of incidents.</li><li>• Ensure awareness of cyber resources, esp. free.</li><li>• Help connect financial resources.</li></ul>
05	<b>Education &amp; Awareness</b>	<ul style="list-style-type: none"><li>• Upskilling and training</li><li>• Recommend MDE &amp; DoIT host tailored training to improve cybersecurity awareness.</li><li>• Leverage universities and water trade groups knowledge and expertise.</li><li>• Certify cybersecurity training programs.</li></ul>



# State of Maryland Cybersecurity Action Plan for Water and Wastewater Systems

Prepared by the Maryland Department of the  
Environment on behalf of the Moore-Miller  
Administration

June 28, 2024



State of Maryland Cybersecurity Action Plan for Water and Wastewater Systems  
June 28, 2024

## EXECUTIVE SUMMARY

The Maryland Cybersecurity Action Plan for Water and Wastewater Systems aims to address critical cybersecurity vulnerabilities within Maryland's water and wastewater infrastructure. This initiative is driven by the urgent need to protect these essential systems from increasingly sophisticated cyber threats, as outlined by recent federal advisories, the Modernize Maryland Act of 2022 (HB1205)<sup>1</sup>, and in direct response to the letter from the White House dated March 21, 2024.<sup>2</sup>

The plan's primary goal is to mitigate high-risk cybersecurity gaps quickly and effectively while setting a foundation for long-term resilience strategy. The increasing frequency and severity of cyberattacks on water and wastewater systems underscore the necessity for immediate action. By leveraging both state and federal resources, this plan seeks to safeguard the public from disruptions to critical water services.

## COVERAGE AND APPLICABILITY

This plan focuses on "covered systems"—those serving over 3,300 people or utilizing Operational Technology (OT) thus targeting the facilities with the highest potential impact on public health and safety if compromised. The State currently lacks the authority to require all covered systems to address cybersecurity. MDE intends to seek the authority to require all covered systems to perform routine cybersecurity assessments and develop and implement risk mitigation and emergency response plans.

## KEY ACTIONS

- 1. Cybersecurity Assessment for Covered Systems-** Compile a list of covered systems by September 1, 2024, notify systems of their obligations by October 1, 2024, and provide guidance for conducting assessments aligned with the NIST Cybersecurity Framework (CSF).

<sup>1</sup> Modernize Maryland Act of 2022,  
[https://legis.maryland.gov/factsheets/factsheet.aspx?docid=2022-0001](#)



# Maryland Water Sector - Community Water Systems

	System Size	Number of Systems	Population Served	Population Percentage	Name	Population Served	Population Percentage
96.5%	Very Large	5	4,181,331	76.19%	WSSC & City of Baltimore	3.5 million	63.77%
	Large	26	888,866	16.20%	City of Hagerstown & Frostburg	933,000	1.88%
3.5%	Medium	40	225,748	4.11%	Town of Mount Airy & Centreville	13,212	0.24%
	Small	105	141,528	2.58%			
	Very Small	292	50,526	0.92%			
	Total	468	5,487,999	100%			

# What SB 871 Accomplishes

- 1) **Cybersecurity Coordination:** Strengthening cybersecurity oversight by designating MDE as the lead regulatory agency and requiring coordination with DoIT and MDEM to establish standards and best practices.
- 2) **Regulatory Updates:** Mandates updated regulations for community water and sewerage systems.
- 3) **Incident Reporting:** Requires water and sewerage systems to report cybersecurity incidents.
- 4) **Stronger Standards:** Ensures systems adopt cybersecurity standards meeting or exceeding those of the Department of Information Technology.
- 5) **Security Protections:** Prohibits public access to critical infrastructure security records.

# ***Cyber Resilience Equals Water Resilience***

**REPORT**- Maryland's Community  
Water and Wastewater Systems:  
Analysis and Recommendations

This report is unanimously supported  
by the Maryland Cybersecurity Council  
Subcommittee on Critical  
Infrastructure



***Cyber Resilience  
Equals  
Water Resilience***

---

Thank you

Questions?



# Why we need increased cybersecurity

## CRITICAL

**“Water is the only utility that you ingest.** So, if a bad actor gets into and wreaks havoc on a water system, the consequences could be very dire”

Jennifer Kocher, VP of Communications and Marketing, the National Water Companies Association

## VULNERABILITY

**Cyberattacks against CWSs are increasing in frequency and severity across the country.**

Based on actual incidents we know that a cyberattack on a vulnerable water system may allow an adversary to manipulate operational technology, which could cause significant adverse consequences for both the utility and drinking water consumers.

U.S. EPA, June 2024

## PRE-SECURITY

Water and wastewater systems in the U.S. are vital to public health and the environment, but they also suffer from chronic underfunding, legacy infrastructure and an expanding attack surface. **The reliance on OT systems, many of which lack modern security protections, has made these utilities particularly susceptible to cyber threats.**

Jonathan Reed, November 4, 2024

## GEOPOLITICS

Critical infrastructure networks worldwide continue to be targeted by malicious cyber actors, including in conflict, where cyberspace is now an established domain of warfare and **cyberattacks are used for strategic, political, economic and national security objectives.**

Australian Signals Directorate

The Maryland state flag is shown waving on a flagpole. It features a yellow and black checkered pattern in the upper left canton, a red and white cross in the center, and a red and white horizontal stripe in the lower half. The background is a blurred blue and white architectural structure.

# Maryland as a Cyber Leader

- Increased cyber threats, recent attacks
- Lack of comprehensive Federal regulation
  - New administration, awaiting cyber leaders
- States encouraged to act independently

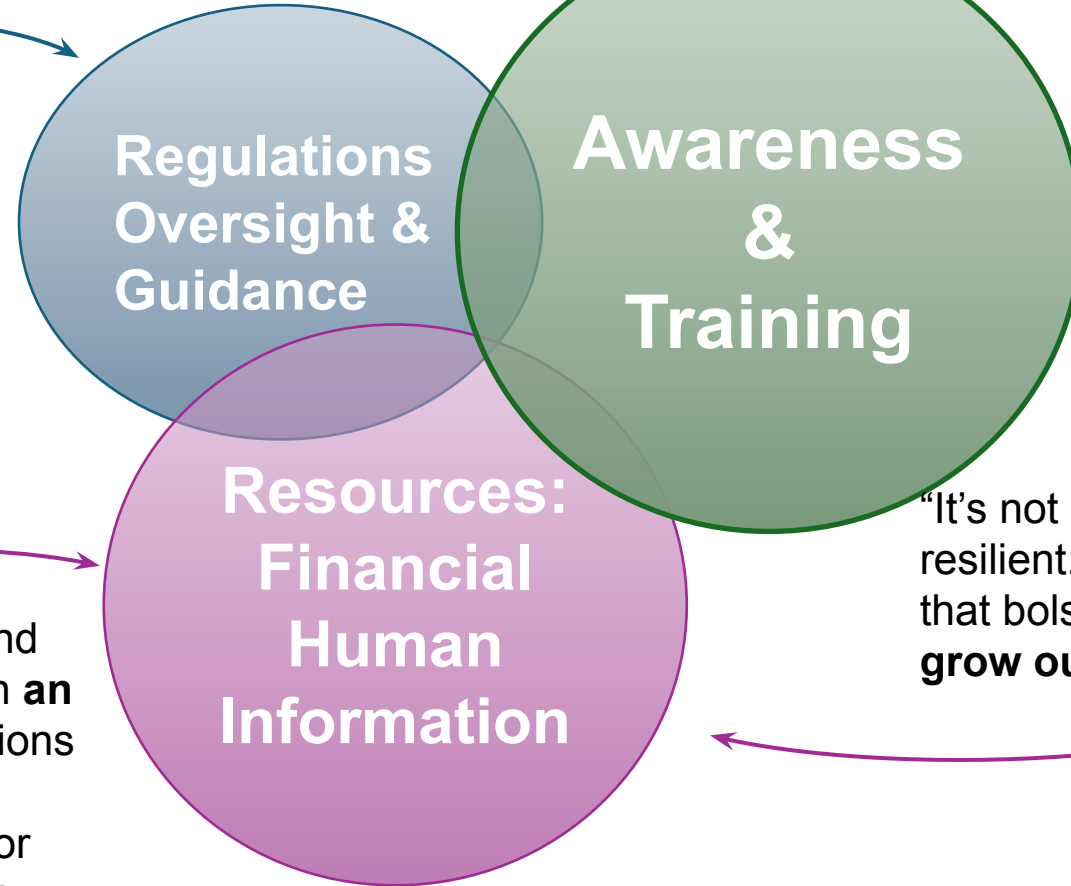
To improve cybersecurity in the U.S. water and wastewater sector, there has been a lot of discussion about improving security. However, **now is the time to take action** to implement security in the sector. We must move beyond the idea of improving security, and act to increase security within our water systems.

--Discussion with Rob M. Lee, CEO of Dragos

# How Do We Increase Security and Resilience?

Matthew Mitroka, PhD, CISSP presented findings and recommendations for the office of the attorney general and the MD Cybersecurity Council.

“Cyber security **legislation and regulation**, such as the new Cyber Security and Resilience Bill, are crucial steps.”



“We need all organizations – public and private – to see cyber security as both **an essential foundation** for their operations and a driver for growth, to view cyber security not just as a ‘necessary evil’ or compliance function but as a business investment, a catalyst for innovation and an integral part of achieving their purpose.”

“It’s not enough any more to talk about being resilient. We must all take the crucial steps that bolster our defences, that **improve and grow our capability** to contest.”

Quotes from UK National Cyber Security Centre CEO Dr Richard Horne, 12/3/2024

# **DoD\_Support\_for\_MD\_HB1062\_Water\_Infrastructure\_Cle**

Uploaded by: John Garstka

Position: FAV





ACQUISITION

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE**  
3600 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3600

CLEARED  
For Open Publication  
Feb 24, 2025

Department of Defense  
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

**February 26, 2025**

**Maryland General Assembly  
House Environment and Transportation Committee  
251 Taylor House Office Building  
Annapolis, Maryland 21401  
Delegate Marc Korman, Chair**

**House Health and Government Operations Committee  
241 Taylor House Office Building  
Annapolis, Maryland 21401  
Delegate Joseline A. Peña-Melnyk, Chair**

**Remarks of  
Mr. John Garstka  
Director, Cyber Warfare  
United States Department of Defense**

**Support of: House Bill 1062 – Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments**

**Testimony**

Chairman Korman, Chairperson Peña-Melnyk, and honorable committee members, the Department of Defense is grateful for the opportunity to support the policies reflected in House Bill 1062.

The Office of the Director of National Intelligence (ODNI), in their 2024 Annual Threat Assessment, highlighted the cyber threat to commercial critical infrastructure posed by China and Russia.<sup>1</sup> (See Figure 1). This document states:

“China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks.”

“If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets.

Furthermore, this threat assessment states:

“Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war.”

---

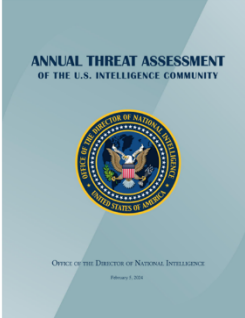
<sup>1</sup> [2024 Annual Threat Assessment of the U.S. Intelligence Community](#)

“Russia maintains its ability to target critical infrastructure, including under water cables and industrial control systems, in the United States as well as in allied and partner nations.

**(U) People's Republic of China**

- (U) "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks."
- (U) "Beijing's cyber espionage pursuits and its industry's export of surveillance, information, and communications technologies increase the threats of aggressive cyber operations against the United States..."
- (U) "If Beijing believed that a major conflict with the United States were imminent, it would consider aggressive cyber operations against U.S. critical infrastructure and military assets."

GRAPHIC IS UNCLASSIFIED



Reference: ODNI Annual Threat Assessment of the USIC 2024

GRAPHIC IS UNCLASSIFIED

**(U) Russia**

- (U) "Russia will pose an enduring global cyber threat even as it prioritizes cyber operations for the Ukrainian war."
- (U) "Moscow views cyber disruptions as a foreign policy lever to shape other countries' decisions and continuously refines and employs its espionage, influence, and attack capabilities against a variety of targets."
- (U) "Russia maintains its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries."

Figure 1. The Cyber Threat is a Clear and Present Danger, 1 of 2

Furthermore, the ODNI released in June of 2024 specific information on cyber attacks on commercial critical infrastructure that took place over a five month period.<sup>2</sup> A third of these attacks by malicious cyber actors were on water and wastewater management, as portrayed in Figure 2. The key take away is that there are a range of malicious cyber actors with the capability and intent to degrade commercial critical infrastructure in the United States. Consequently, the new reality is that commercial critical infrastructure providers need to be capable of operating in a contested cyberspace environment.

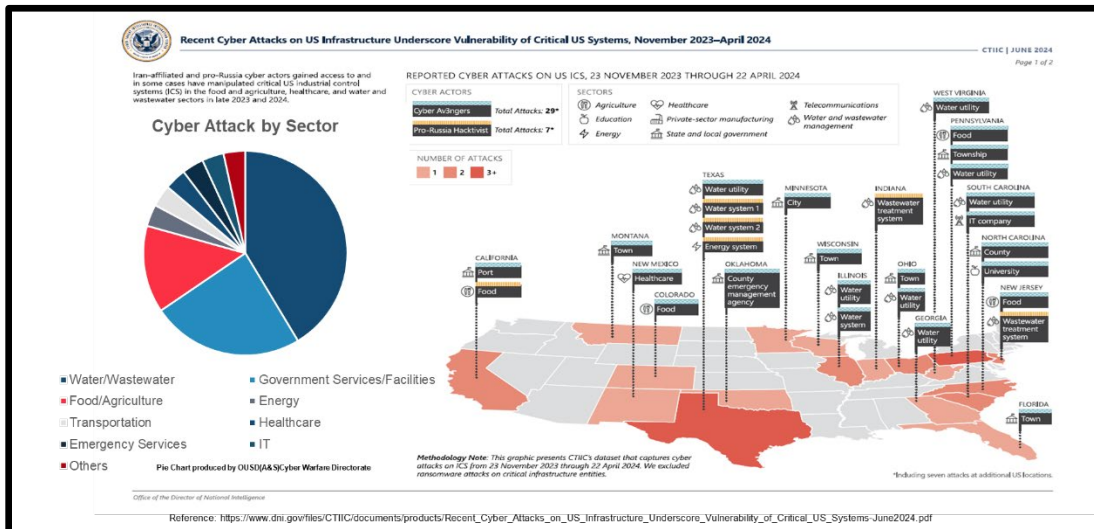


Figure 2. The Cyber Threat is a Clear and Present Danger, 2 of 2

<sup>2</sup>[https://www.dni.gov/files/CTIIC/documents/products/Recent\\_Cyber\\_Attacks\\_on\\_US\\_Infrastructure\\_Underscore\\_Vulnerability\\_of\\_Critical\\_US\\_Systems-June2024.pdf](https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf)

The Department of Defense is dependent upon commercial critical infrastructure to develop capabilities for the Joint Force and to conduct military operations. This relationship is portrayed in the mission stack, as portrayed in Figure 3.

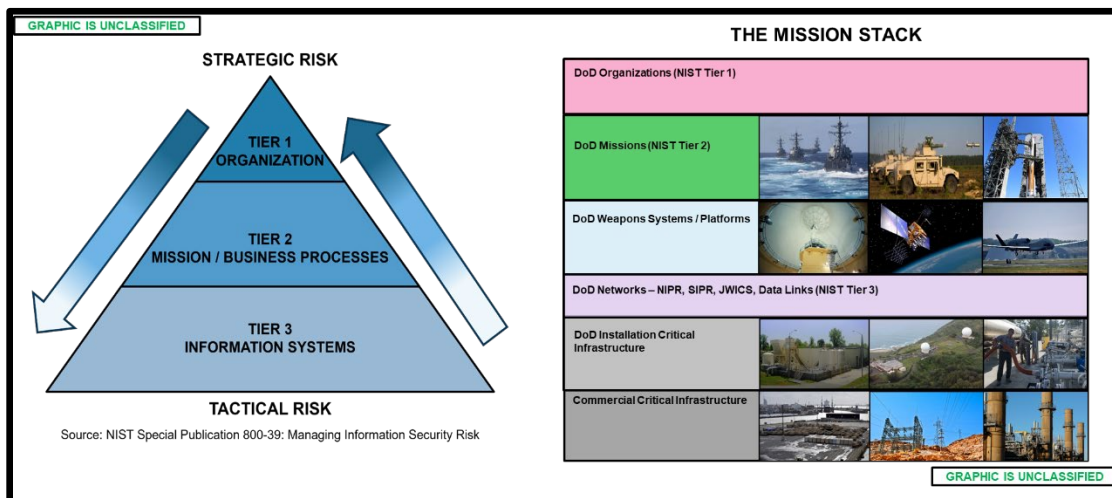


Figure 3. The Mission Stack

National Security Memorandum 22 and DoD policy guidance have highlighted the importance of securing commercial critical infrastructure upon which the Department of Defense and other Federal Agencies depend on to conduct their missions<sup>3</sup>.

Specifically, DoD’s guidance has highlighted the importance of working with State and Local governments to help bolster the cybersecurity of commercial critical infrastructure supporting DoD’s ability to conduct its mission.

The newly appointed Secretary of Defense highlighted as one his three priorities “Restoring Deterrence.” In the current threat environment, **Cybersecurity is a key element of Deterrence.**

The Department in its Fiscal Year 2024 budget allocated over \$250M to cyber harden installation critical infrastructure (e.g, water, fuel, power) on DoD installations that support priority DoD missions. Additionally, the Department has recently developed an increased understanding of the challenges that small and medium sized businesses face in improving their cybersecurity posture. We are applying this insight to explore options for bending the cybersecurity cost curve to help companies that the Department is dependent upon improve their cybersecurity posture.

<sup>3</sup> National Security Memorandum 22: National Security Memorandum on Critical Infrastructure Security and Resilience, April 2024.

There is an emerging understanding that the Department must play a role in cyber hardening priority commercial critical infrastructure that the DoD depends on to conduct its missions. To accomplish this objective, DoD needs to work closely with State and Local governments. The state of Maryland hosts, at least, 9 major military installations that support a range of important DoD missions. All of these DoD installations are dependent upon water provided by the commercial providers in the State of Maryland (See Figure 4).

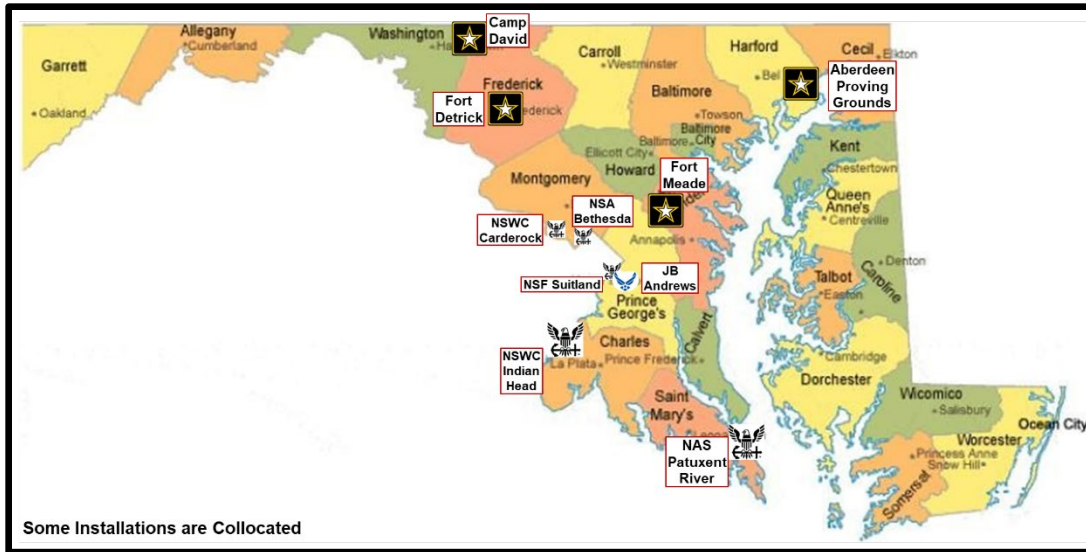


Figure 4. Major Military Installations in Maryland (not all inclusive)

The legislation being proposed by Senator Hester in House Bill 1062 will enhance the cybersecurity posture of water providers and enhance the ability of state of Maryland to operate in a contested cyberspace environment. This legislation will improve the safety and availability of the water supply for residents of the State of Maryland and help secure the water supply that DoD installations depend on. This legislation will improve the overall cybersecurity posture of the State of Maryland and in doing so will contribute in a meaningful way to National Security.

Yours etc.,

John J. Garstka  
Director, Cyber Warfare

# **HB 1062 Written Testimony \_ Maryland Military Coal**

Uploaded by: Lynn Nash

Position: FAV



# MARYLAND MILITARY COALITION

*Serving Veterans through Legislative Advocacy*

February 26, 2025

The Honorable Mark Korman  
The Honorable Regina T. Boyce  
House Environment and Transportation Committee  
250 Taylor House Office Building  
6 Bladen Street  
Annapolis, MD 21401

Subject: Request for a **Favorable Report – HB1062 Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments**

Dear Chair Korman, Vice Chair Boyce and Distinguished Members of the Environment and Transportation Committee:

On behalf of the Maryland Military Coalition, and as the former Senior Public Health Advisor to the Secretary of the Department of Homeland Security, I write to recommend a **Favorable Report – HB1062 Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments**. This bill is intended to “harden” community water and sewage systems from the threat of cybersecurity breaches that could disrupt operations over a prolonged time. Specifically the legislation requires that community water and sewage system providers undertake recommended cybersecurity measures to ensure that systems, communications and information are protected against damage, unauthorized use or modification and exploitation, as well as a requirement to report cybersecurity incidents. Cybersecurity recommendations include awareness, training, best practices, and plans for disruption of service due to cyber incidents including ransomware attacks including alternative water supplies and mutual aid agreements when water supplies are compromised. Seminal to these efforts is provider participation in the Maryland Information Sharing and Analysis Center and an annual table top exercise.

Secure water and sewage services are essential to life in both civilian and military communities. The bill’s requirement for coordination among the Department of the Environment, Department of Information Technology, and Maryland Department of Emergency Management reflects both the Departments of Homeland Security and Defense’s emphasis on partnering with state and local entities to secure critical infrastructure. The bill’s proactive cybersecurity standards and incident reporting requirements are critical steps to mitigate these threats.

Request for a **Favorable Report – HB1062 Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments**

Passage of this bill is necessary because in 2024 alone, there were **FIVE cybersecurity events involving water or water treatment plants in the United States:**

1. **Veolia North America. January 2024.** The company operates 8,500 water and wastewater facilities around the world, as well as in all 50 US states. Online bill payment systems were infiltrated with theft of personally identifiable information. Veolia took targeted back-end systems and servers offline as a defensive measure. Customers experienced delays using the online bill payment systems as a result of this action. Water or wastewater treatment operations did not appear to have been impacted.
2. **Texas Cities: Hale Center, Muleshoe, Lockney and Abernathy. January 2024.** Multiple water and wastewater plants in Texas, United States, were hit by cyber-attacks in early 2024. Videos posted online by the purported hackers showed them interacting with various supervisory control and data acquisition (SCADA) systems remotely, arbitrarily adjusting settings and controls. The common link was the vendor software used by the communities. In most cases suspicious activity was caught before material damage was caused, although in one city, a water tank overflowed for more than 30 minutes until operations switched to manual control while steps were taken to resecure systems. The attacks were attributed to a Russia-linked group.
3. **Tipton, Indiana, April 2024.** The Cyber Army of Russia posted a video online showing how hackers allegedly interacted with the systems of the Tipton Wastewater Treatment Plant. Facility staff noticed irregular activity through standard process monitoring of plant operations, and transitioned systems to manual control while the matter was investigated.
4. **Arkansas City Water Treatment Facility, September 2024.** The water treatment facility in Arkansas City, Kansas, experienced a cybersecurity incident on 22 September 2024, leading to a temporary switch to manual operations. Despite the incident, there was no disruption to the water supply or service delivery. Enhanced security measures were implemented, and authorities were involved to resolve the situation.
5. **American Water, October 2024.** Week-long outage of billing and customer account systems. The attack, discovered on 3 October 2024, led to the shutdown of the company's call center and rescheduling of customer appointments. Despite these disruptions, water and wastewater facilities were not impacted. The company, serving 14 million people, paused billing and took measures to protect systems and data.

Likely ***there were more incidents*** in the United States, as most companies prefer not to publicly report their incidents.

Request for a **Favorable Report – HB1062 Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments**

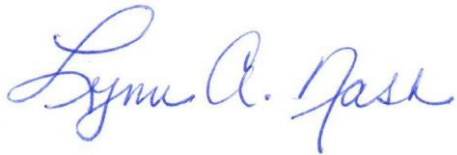
The policies in HB 1062/ SB 871 focus on strengthening cybersecurity for community water and sewerage systems, which are vital to civilian communities, military bases, personnel, and their families. The information-sharing mechanisms between state and local governments and our 20 Maryland military bases improve situational awareness and unify cybersecurity strategies across government levels.

For these reasons, the Maryland Military Coalition **STRONGLY** supports a **HB1062 Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments** and asks you for a **FAVORABLE Report**.

The Maryland Military Coalition is a registered non-profit, non-partisan advocacy organization comprised of 22 prominent Maryland-based veteran and military groups, representing over 150,000 service-connected individuals, including those currently serving, veterans, retirees and their families, caregivers, and survivors.

We wish to thank Delegate Harrison for her on-going support of **ALL** of the uniformed services community in Maryland.

Respectfully,



Lynn A. Nash  
CAPT (R), U.S. Public Health Service  
Communications Director







## Member Organizations of the Maryland Military Coalition

Air Force Sergeants Association

American Military Society

American Minority Veterans Research Project

Association of the United States Navy

Commissioned Officers Association of the U.S. Public Health Service

Disabled American Veterans

Fleet Reserve Association of Annapolis

Jewish War Veterans of the U.S.A

Maryland Air National Guard Retirees' Association

Maryland Veterans Chamber of Commerce

Military Officers Association of America

Military Order of the Purple Heart

Military Order of the World Wars

Montford Point Marines of America

National Association of Black Veterans

National Association of Retired Federal Employees, Maryland Veterans

Naval Enlisted Reserve Association

NOAA Association of Commissioned Officers

Platoon 22

Reserve Organization of America

Society of Military Widows

Veterans of Foreign Wars

**HB 1062 - FWA - MDEM.pdf**

Uploaded by: Anna Sierra

Position: FWA



[mdem.maryland.gov](https://mdem.maryland.gov)

877-636-2872

7229 Parkway Drive, Suite 200 | Hanover, MD 21076

Governor | Wes Moore Lt. Governor | Aruna Miller Secretary | Russell J. Strickland

**Favorable with Amendments - HB 1062**  
**Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments**  
Environment and Transportation Committee  
Hearing Date: 26 February 2025

The Maryland Department of Emergency Management (MDEM) writes today in support with amendments of **HB 1062 Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments**.

**HB 1062** is a complex bill that would require the Cyber Preparedness Unit within MDEM to provide direct planning support to community water and sewerage systems, develop risk communications plans, and conduct an annual tabletop exercise.

The Department acknowledges the risks posed by cyber attacks on various sectors in Maryland. The Cyber Preparedness Unit was established in part to work closely with local governments to plan for these attacks, and MDEM agrees that planning, training, and exercising are key elements to increasing preparedness in Maryland. However, local governments have the primary authority for responding to emergencies in their communities, including impacts to community water systems and issuing public information and warnings. Private entities are responsible for conducting their own planning, training, and exercises, and both local and State governments often participate in these efforts under a whole community approach to preparedness.

MDEM's amendments to the bill, outlined below, reflect this standard by shifting the Department's focus from interacting directly with community water systems to providing local emergency management organizations with guidance related to these efforts. The Department consulted with the MACo Emergency Management affiliate, MDE, and DoIT in the development of these amendments.

#### **Amendment 1**

Page 5, Lines 3-6. Replace "Maryland Department of Emergency Management" with "local emergency manager." Community water systems should be communicating directly with the local emergency manager before, during, and after emergencies. As local governments need support, they request that support from MDEM.

#### **Amendment 2**

Page 8, Lines 25-28. Re-phrase to, “Providing guidance to local emergency management organizations for incidents against water and wastewater facilities.” In Maryland’s tiered emergency management system, MDEM provides planning support and technical assistance at the request of county emergency management agencies and does not plan directly for private sector entities.

**Amendment 3**

Page 9, Lines 5-7. Strike the provision. In coordination with emergency management stakeholders, the Department develops an annual integrated preparedness plan which outlines training and exercises to be conducted each year. This plan is a federal requirement and reflects the ever-changing threat and hazard landscape. It is not best practice to establish a hazard-specific, permanent exercise requirement in law as it provides limited flexibility to the Department to use other scenarios which may be a higher risk in a given year.

**Amendment 4**

Page 9, Lines 8-10. Rephrase to, “Develop guidance for crisis and emergency risk communication for local emergency management organizations in the State.” Local emergency management organizations are the lead authority for public information and warning. MDEM recommends instead providing guidance for public information and warning.

**Amendment 5**

Page 10, Line 3. Strike “Know the Threats” to ensure MDEM has flexibility to change website headings and page names as needed.

**Amendment 6**

Page 10, Lines 4-5. Strike. The Department prefers to retain flexibility to use the best possible public alert and warning system. MDRReady is already in use and managed by the Department, and codification will only limit the Department’s future flexibility in using other systems as appropriate.

We are aware that in addition to our amendments, MDE and DoIT also have proposed amendments to this legislation. MDEM fully supports those amendments offered by our sister agencies.

In conclusion, the Maryland Department of Emergency Management respectfully requests a favorable report with the amendments proffered by the Department as well as MDE and DoIT on **HB 1062**. If you have any questions, please contact Anna Sierra, MDEM legislative liaison: [anna.sierra1@maryland.gov](mailto:anna.sierra1@maryland.gov).

**HB1062-ET\_MACo\_SWA.pdf**

Uploaded by: Dominic Butchko

Position: FWA



## House Bill 1062

*Department of the Environment - Community Water and Sewerage Systems -  
Cybersecurity Planning and Assessments*

MACo Position: **SUPPORT**  
**WITH AMENDMENTS**

To: Environment & Transportation and  
Health & Government Operations Committees

Date: February 26, 2025

From: Karrington Anderson and Dominic J. Butchko

The Maryland Association of Counties (MACo) **SUPPORTS** HB 1062 **WITH AMENDMENTS**. This bill seeks to strengthen cybersecurity protections for public water and wastewater systems by requiring a Zero-Trust security model, annual third-party cybersecurity assessments, and certification of compliance with cybersecurity standards. While counties recognize the importance of cybersecurity enhancements, the mandated requirements in this bill pose significant financial and operational challenges for local governments.

Counties take cybersecurity seriously and follow established frameworks such as the NIST Cybersecurity Framework and the Criminal Justice Information Systems (CJIS) Security Policy. However, HB 1062 would require substantial upgrades to county IT infrastructure, including costly network restructuring, additional licensing, firewall reconfiguration, and ongoing maintenance. Many county IT directors acknowledge Zero-Trust as a long-term goal, but the transition requires significant investment. Compliance with annual third-party assessments is another major concern. While external assessments provide valuable insights, they are costly, and many counties rely on free assessments from CISA, which have long waitlists. Compliance with HB 1062 would place an untenable fiscal burden on counties already struggling with workforce shortages and hiring freezes, making it extremely difficult to allocate the necessary resources for additional cybersecurity staff and administration.

For example, Calvert County estimates that compliance costs would total approximately \$1.6 million for FY26 and similarly for FY27, with ongoing annual costs of \$840,000 annually from FY28 to FY30. To ensure that counties can enhance cybersecurity in a financially sustainable manner, MACo urges amendments to shift the bill's mandates to best practices, allowing counties the flexibility to implement cybersecurity measures based on risk assessments and available funding. Additionally, State resources or grants could be provided to assist with the costs of compliance.

Counties fully support stronger cybersecurity for water and wastewater systems, but the fiscal and operational burdens of HB 1062 must be addressed. For these reasons, MACo urges a **FAVORABLE WITH AMENDMENTS** report on HB 1062.

**MDE HB1062 SWA.pdf**

Uploaded by: Jeremy D. Baker

Position: FWA





**The Maryland Department of the Environment  
Secretary Serena McIlwain**

***House Bill 1062***

***Department of the Environment - Community Water and Sewerage Systems - Cybersecurity  
Planning and Assessments***

**Position:** Support with Amendments  
**Committee:** Environment and Transportation  
**Date:** February 26, 2025  
**From:** Alex Butler, Deputy Director of Government Relations

---

The Maryland Department of the Environment (MDE) **SUPPORTS HB 1062 WITH AMENDMENTS.**

**Bill Summary**

House Bill 1062 requires community water and sewerage systems develop and implement comprehensive cybersecurity plans. The covered systems must also conduct regular assessments to identify and mitigate potential cyber threats.

**Position Rationale**

Cyberattacks against Maryland's water and sewerage infrastructure can at a minimum disrupt the delivery of core public services and at a maximum threaten public health and safety. House Bill 1062 is critical for enhancing our security and resilience. By requiring these systems to adopt and maintain robust cybersecurity measures, the bill aims to protect water and sewerage services from potential disruptions caused by cyber incidents. Implementing the bill's provisions will necessitate collaboration among various stakeholders, including state agencies, local governments, and private entities, to ensure effective cybersecurity practices are adopted and maintained across all community water and sewerage systems.

Maryland developed a Cybersecurity Action Plan for Water and Wastewater Systems in 2024 which was reviewed at the federal level by the National Security Council. House Bill 1062 generally aligns with the recommended actions described by that plan.

MDE is offering the attached amendments to clarify certain notice, assessment, and enforcement requirements. MDE has also consulted with the Maryland Department of Information Technology and the Maryland Department of Emergency Management and supports the amendments those agencies are offering.

For the reasons detailed above, MDE requests a **FAVORABLE WITH AMENDMENTS** report for HB 1062.

**Contact:** Alex Butler, Deputy Director of Government Relations  
Email: [alex.butler@maryland.gov](mailto:alex.butler@maryland.gov)

## Amendments

### AMENDMENT NO. 1

On page 5, in line 20, strike “SIMILAR TO” and substitute “MODELED AFTER”.

### AMENDMENT NO. 2

On page 5, in line 24, strike “EACH” and substitute “EVERY OTHER”.

### AMENDMENT NO. 3

On page 6, strike beginning with “STANDARDS” in line 5 down through “UNDER” in line 6; in the same line, strike “(4)”; in the same line, after “subtitle” insert a semicolon; strike line 7 in its entirety; and in line 9, after “DESIGNEE” insert “; AND

**(3) NOTIFY THE DEPARTMENT OF ANY NON-COMPLIANCE WITH § 9-2705(B) OF THIS SUBTITLE**”.

### AMENDMENT NO. 4

On page 6, in line 23, after “TECHNOLOGY” insert “OR OPERATING TECHNOLOGY”.

### AMENDMENT NO. 5

On page 7, after line 17 insert:

**“9-2708.**

**A PERSON WHO VIOLATES THE PROVISIONS OF THIS SUBTITLE, ANY REGULATION ADOPTED UNDER THIS SUBTITLE, OR ANY ORDER ISSUED UNDER THIS SUBTITLE SHALL BE SUBJECT TO THE PROVISIONS OF §§ 9-334 THROUGH 9-344 OF THIS TITLE.”**

# House Bill 1062 - DoIT Written Testimony.docx.pdf

Uploaded by: Sara Elalamy

Position: FWA



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

**TO:** House Environment and Transportation Committee  
**FROM:** Department of Information Technology  
**RE:** House Bill 1062 - Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments  
**DATE:** February 26, 2025  
**POSITION:** Support with Amendments

---

The Honorable Marc Korman  
House Environment and Transportation Committee  
250 Taylor House Office Building  
Annapolis, Maryland 21401

Dear Chairman Korman,

The Department of Information Technology (DoIT) supports House Bill 1062 - Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments with amendments. This bill aims to strengthen Maryland's water and wastewater infrastructure against cyber threats through regulatory oversight, training, and enhanced security measures.

DoIT supports HB 1062 with amendments and is fully aligned with the amendments put forth by the Maryland Department of Environment (MDE) and the Maryland Department of Emergency Management (MDEM). We respectfully request that all proposed amendments be incorporated into the final legislation to ensure a comprehensive and effective implementation of the bill's objectives. Specifically, DoIT has the following amendment recommendations:

- We recommend that the cybersecurity standards referenced in the bill align with the existing State Minimum Cybersecurity Standards, rather than adopting independent criteria that may cause inconsistencies in regulatory compliance.
- We propose that the Maryland Department of the Environment (MDE) be responsible for collecting cybersecurity compliance certifications from community water and sewerage systems, as this function does not require direct cybersecurity expertise.
- The requirement for DoIT to analyze and report on cybersecurity technology and policies should be reconsidered, given that without additional investment in oversight, such reporting may not provide meaningful insights into security improvements.
- The bill should streamline cybersecurity incident reporting requirements to avoid



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

conflicting language across sections. We suggest that all reporting be aligned under a single, clear directive referencing DoIT's established guidance.

DoIT stands ready to support the implementation of HB 1062; however, it is important to recognize that successful execution of this program will require additional resources. Specifically, we estimate that at least **\$225,000 per fiscal year** will be necessary to hire an expert in the field to properly manage and oversee the cybersecurity initiatives outlined in the bill. Without this dedicated expertise, the ability to provide meaningful oversight and assistance to community water and sewerage systems may be significantly hindered.

Once again, we appreciate your leadership and commitment to strengthening Maryland's cybersecurity posture. We urge the adoption of our amendments, as well as those proposed by MDE and MDEM, to ensure the effectiveness of HB 1062.

Best,

Melissa Leaman  
Acting Secretary  
Department of Information Technology

**MML-HB 1062-UNFAV.pdf**

Uploaded by: Iris Ibegbulem

Position: UNF



Maryland Municipal League  
*The Association of Maryland's Cities and Towns*

## TESTIMONY

February 24, 2025

**Committee:** House Environment and Transportation

**Bill:** HB 1062 - Department of the Environment - Community Water and Sewerage Systems - Cybersecurity Planning and Assessments

**Position:** Unfavorable

**Reason for Position:**

The Maryland Municipal League (MML) respectfully requests an unfavorable report for House Bill 1062 which seeks to enhance cybersecurity systems on county and municipal water and sewage systems. The Maryland Municipal League consists of 161 municipalities, towns, villages, and cities, all with varied needs for their water and sewage structures. House Bill 1062 requires regular assessments and reporting to ensure that these water and sewage systems are compliant with the standards needed. With these assessments starting at thousands of dollars, annual assessments or even assessments every 2 years would become a substantial financial burden on many municipalities.

With regard to House Bill 1062, implementing a Zero Trust cybersecurity model would mean restructuring any municipal network. This new model could take many years to complete and drain already limited local government resources. In totality, this bill would impose fiscal strain with the need for additional human capital and commitment to technological upgrades, the likes of which many municipalities simply cannot afford.

It is because of these reasons that the Maryland Municipal League requests an unfavorable report on HB 1062. For more information, please contact Iris Ibegbulem, Senior Associate, Advocacy and Public Affairs at [irisi@mdmunicipal.org](mailto:irisi@mdmunicipal.org) or 443-295-9457. Thank you in advance for your consideration.

*The Maryland Municipal League uses its collective voice to advocate, empower and protect the interests of our 160 local governments members and elevates local leadership, delivers impactful solutions for our communities, and builds an inclusive culture for the 2 million Marylanders we serve.*

**MAMWA Ltr HB 1062 2.24.25.pdf**

Uploaded by: Lisa Ochsenhirt

Position: UNF





## Maryland Association of Municipal Wastewater Agencies, Inc.

Washington Suburban Sanitary Commission

14501 Sweitzer Lane, 7<sup>th</sup> Floor

Laurel, MD 20707

Tel: 301-206-7008

### MEMBER AGENCIES

Allegany County  
Anne Arundel County  
City of Baltimore  
Baltimore County  
Town of Berlin  
Cecil County  
Charles County  
City of Cumberland  
D.C. Water  
Frederick County  
City of Hagerstown  
Harford County  
City of Havre de Grace  
Howard County  
Ocean City  
Pocomoke City  
Queen Anne's County  
City of Salisbury  
Somerset County Sanitary District  
St. Mary's Metro. Comm.  
Washington County  
WSSC Water

February 24, 2025

The Honorable Marc Korman  
Chair, House Environment and Transportation Committee  
250 Taylor House Office Building  
Annapolis, MD 21401

### Re: **OPPOSE -- HB 1062 (Department of the Environment – Community Water and Sewerage Systems – Cybersecurity Planning and Assessments)**

Dear Chair Korman:

On behalf of the Maryland Association of Municipal Wastewater Agencies (MAMWA), I am writing to **OPPOSE HB 1062**, which would, among other things, require any water or wastewater provider that serves over 3,300 customers to comply with cybersecurity standards established by the Maryland Department of the Environment (MDE) (p. 5, l. 17-19), adopt a zero-trust cybersecurity approach for on-premises and cloud-based services (p. 5, l. 20-23), and annually hire a third-party to assess the operational technology and information technology devices in place for the water or wastewater system (p. 5, l. 24-29). MAMWA is a statewide association of local governments and wastewater treatment agencies that serve approximately 95% of the State's sewered population.

HB 1062 is well-intended. Cybersecurity is a critical issue for water and wastewater systems and one that MAMWA members take very seriously. However, MAMWA opposes HB 1062 because it could be destructive to our systems and would be very expensive for our ratepayers.

MAMWA's top priority is the viability of our systems. We are concerned that penetration testing (PEN testing) could damage a utility's SCADA (supervisory control and data acquisition) system, which is at the heart of a water distribution and wastewater treatment system. We are also apprehensive about allowing a "white hat" to review these mission critical systems without a security clearance and a demonstrated knowledge of the exact type of equipment and software being used. Because there are so many types of hardware and software being used, finding competent assistance would be challenging. Lastly, MAMWA strongly objects to any type of storage of or reporting of vulnerabilities.

From a financial perspective, requiring a zero-trust cybersecurity approach, although a worthy goal, would mean connecting any stand-alone water and wastewater computer systems to the larger county or municipal system. This would be a considerable undertaking requiring additional employees, a complete overhaul of the larger system's

### CONSULTANT MEMBERS

Black & Veatch  
GHD Inc.  
Hazen & Sawyer  
HDR Engineering, Inc.  
Jacobs  
Ramboll Americas  
WRA

### GENERAL COUNSEL

AquaLaw PLC

MAMWA Letter on HB 1062

February 24, 2025

Page 2

firewalls, and upgrades to existing licenses. Hiring a third-party consultant to annually assess the system would cost between \$30,000 to \$40,000 per review.

MAMWA urges the Committee to **Vote NO** on HB 1062.

Please feel free to contact me with any questions at [Lisa@AquaLaw.com](mailto:Lisa@AquaLaw.com) or 804-716-9021.

Sincerely,



Lisa M. Ochsenhirt  
MAMWA Deputy General Counsel

cc: Environment and Transportation Committee Members, HB 1062 Sponsor